

RADC-TR-88-89, Vol I (of two)
Final Technical Report
March 1988



4

AD-A200 204

DTIC FILE COPY

R/M/T DESIGN FOR FAULT TOLERANCE, PROGRAM MANAGER'S GUIDE

Grumman Aerospace Corporation

David J. Conroe and Stanley J. Murn, Jr.



APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

ROME AIR DEVELOPMENT CENTER
Air Force Systems Command
Griffiss Air Force Base, NY 13441-5700

88 8 19 004

This report has been reviewed by the RADC Public Affairs Division (PA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

RADC-TR-83-69, Volume I (of two) has been reviewed and is approved for publication.

APPROVED:

Joseph A. Caroli
JOSEPH A. CAROLI
Project Engineer

APPROVED:

Raymond C. White
RAYMOND C. WHITE, Colonel, USAF
Director of Reliability & Compatibility

FOR THE COMMANDER:

John A. Ritz

JOHN A. RITZ
Directorate of Plans & Programs

If your address has changed or if you wish to be removed from the RADC mailing list, or if the addressee is no longer employed by your organization, please notify RADC (RBET) Griffiss AFB NY 13441-5700. This will assist us in maintaining a current mailing list.

Do not return copies of this report unless contractual obligations or notices on a specific document require that it be returned.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED			1b. RESTRICTIVE MARKINGS N/A		
2a. SECURITY CLASSIFICATION AUTHORITY N/A			3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution unlimited.		
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A					
4. PERFORMING ORGANIZATION REPORT NUMBER(S) N/A			5. MONITORING ORGANIZATION REPORT NUMBER(S) RADC-TR-88-69, Volume I (of two)		
6a. NAME OF PERFORMING ORGANIZATION Grumman Aerospace Corporation		6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION Rome Air Development Center (RBET)		
6c. ADDRESS (City, State, and ZIP Code) Aircraft Systems Division S. Oyster Bay Road Bethpage NY 11714			7b. ADDRESS (City, State, and ZIP Code) Griffiss AFB NY 13441-5700		
8a. NAME OF FUNDING/SPONSORING ORGANIZATION Rome Air Development Center		8b. OFFICE SYMBOL (If applicable) RBET	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER F30602-85-C-0161		
8c. ADDRESS (City, State, and ZIP Code) Griffiss AFB NY 13441-5700			10. SOURCE OF FUNDING NUMBERS		
			PROGRAM ELEMENT NO. 62702F	PROJECT NO. 2338	TASK NO. 02
			WORK UNIT ACCESSION NO. 2F		
11. TITLE (Include Security Classification) R/M/T DESIGN FOR FAULT TOLERANCE, PROGRAM MANAGER'S GUIDE					
12. PERSONAL AUTHOR(S) David J. Conroe, Stanley J. Murn, Jr.					
13a. TYPE OF REPORT Final		13b. TIME COVERED FROM Oct 85 TO May 86		14. DATE OF REPORT (Year, Month, Day) March 1988	
				15. PAGE COUNT 166	
16. SUPPLEMENTARY NOTATION RADC-TR-88-69, Volume II (of two) will be published at a later date.					
17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)		
FIELD	GROUP	SUB-GROUP	Reliability Fault Tolerance		
13	08		Maintainability Program Management		
			Testability Design Guidance		
19. ABSTRACT (Continue on reverse if necessary and identify by block number)					
<p>Fault tolerance has come into almost universal use in modern day systems of all types. This report contains design guidance and general information for Air Force and contractor program managers with respect to the nature and form of Reliability, Maintainability/Testability (R/M/T) tasks needed in the development of fault tolerant systems. This program managers guide contains instructions for tailoring the R/M/T programmatic standards (MIL-STDs 785, 470 & 2165) for fault tolerant systems development. Important fault tolerance design options and tradeoff analysis methods are discussed to aid the program manager in understanding and overseeing the entire fault tolerant system design process. This report is Volume I of II. Volume II will be an R/M/T Fault Tolerant Design Implementation Guide available at a later date, and will contain a more in-depth view of the technical issues regarding fault tolerance design techniques.</p> <p>→ Keywords: Com and control communications and intelligence systems, (cdc)</p>					
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT <input checked="" type="checkbox"/> UNCLASSIFIED/UNLIMITED <input type="checkbox"/> SAME AS RPT. <input type="checkbox"/> DTIC USERS			21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED		
22a. NAME OF RESPONSIBLE INDIVIDUAL Joseph A. Caroli			22b. TELEPHONE (Include Area Code) (315) 330-4205		22c. OFFICE SYMBOL RADC (RBET)

DD Form 1473, JUN 86

Previous editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

A

EXECUTIVE SUMMARY

This Program Manager's Guide was prepared by the Aircraft Systems Division of the Grumman Corporation under RADC contract F30602-85-C-0161, entitled *Reliability/Maintainability/Testability (R/M/T) Design for Fault Tolerance*. The objectives of this document are to provide Air Force and contractor program managers with guidance on how to address fault tolerant design issues and needs, and to provide general information on state-of-the-art R/M/T fault tolerance techniques. A *R/M/T Fault Tolerant Design Implementation Guide*, which will contain a more in-depth technical treatise on fault tolerance techniques and analyses methodologies for use by the Air Force and contractor technical personnel, is also being prepared under this contract and will be available by the end of 1988. These Guides are being developed to structure cost effective programs for reliable, maintainable and testable fault tolerant C³I (Command, Control, Communications and Intelligence) systems.

When properly applied, fault tolerance can significantly and effectively enhance the mission capabilities of C³I systems. It is imperative, however, that program managers understand the configuration selection process to avoid the infusion of unnecessary system complexities that contribute little to mission capability and increase life-cycle cost. The system performance, supportability and cost of competing fault tolerance approaches must be clearly defined early in the development phase to support critical management configuration decisions.

This Program Manager's Guide provides the essential background information needed by Air Force and contractor program managers to understand the specification, design and tradeoff analyses required for

fault tolerant C³I system developments. It is organized in a manner that follows the configuration development process and addresses the following critical areas:

- o R/M/T program planning and management
- o Specification of fault tolerance and R/M/T requirements
- o Relationship of fault tolerance to mission and safety criticality
- o Guidance for design of fault tolerance
- o Evaluation of design cost effectiveness.

This Guide can be used either as a tutorial aid or a management reference document. Numerous fault tolerance examples are presented which illustrate the potential benefits that can be derived and areas of application. Graphics and emphasized type fonts are used extensively in this guide to summarize the material presented and to highlight important management issues. In addition, checklists are located at the end of each section. These checklists provide a handy reference of major pertinent R/M/T impact areas that program managers should address in future fault tolerant C³I development programs.

PREFACE

This Program Manager's Guide was prepared by Grumman Aircraft Systems Division Reliability, Maintainability and Safety Section, Bethpage, New York for Rome Air Development Center, Griffiss Air Force Base, New York. Mrs. Heather Dussault and Mr. Joseph Caroli (RBET) were the RADC Project Engineers.

This Guide was developed during the period between September 1985 through March 1987. In addition to the authors, David Conroe and Stanley Murn, Jr., other Grumman study team contributors were Messrs. Gary Bigel, Allan Dantowitz, John DiLeo, Theodore Gordan, Kenneth Haller, John Kappler, Robert Messina, Victor Pellicione, George Pflugel and Edward Ramirez.

Accession for	
NTIS CRA&I	<input checked="checked" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution /	
Availability Codes	
Dist	Avail and/or Special
A-1	



CONTENTS

Section		Page
1	INTRODUCTION	1-1
2	R/M/T PROGRAM PLANNING AND MANAGEMENT	2-1
	2.1 System Tailored Approach	2-1
	2.1.1 Reliability Program Tailoring	2-4
	2.1.2 Maintainability Program Tailoring	2-12
	2.1.3 Testability/Diagnostic Program Tailoring	2-20
	2.1.4 Software Program Tailoring	2-31
	2.2 Program Planning and Management Checklist Questions	2-36
	2.3 Specification of Fault Tolerance and R/M/T Requirements	2-37
	2.3.1 System Quantitative R/M/T Requirements	2-38
	2.3.2 Verification	2-50
	2.3.3 Warranties	2-53
	2.4 Specification Checklist Questions	2-55
3	RELATIONSHIP OF C ³ I FAULT TOLERANCE TO MISSION AND SAFETY CRITICALITY	3-1
	3.1 Formulation of C ³ I Fault Tolerance Requirements	3-1
	3.2 Examples of Typical C ³ I Fault Tolerance Applications	3-6
	3.2.1 Space Surveillance System	3-6
	3.2.2 Airborne Surveillance Radar System	3-12
	3.3 Fault Tolerance Requirements Checklist	3-16

CONTENTS (contd)

Section		Page
4	GUIDANCE FOR DESIGN OF FAULT TOLERANCE.	4-1
4.1	Hardware and Software Fault Tolerance Design	
	Options	4-1
4.1.1	Redundancy Techniques	4-4
4.1.2	Active Redundancy	4-8
4.1.3	Standby Redundancy	4-14
4.1.4	Voting Redundancy	4-15
4.1.5	Hybrid Redundancy	4-16
4.1.6	K of N Configurations	4-17
4.1.7	Graceful Degradation	4-18
4.1.8	Fault Detection Techniques	4-20
4.1.9	Error Detection Codes	4-21
4.1.10	Distributed Processing	4-21
4.1.11	Hardware and Software Fault Tolerant Design Checklist Questions	4-24
4.2	Maintainability/Testability Impact on Fault Tolerant Design Options	4-25
4.2.1	Testability of Fault Tolerant Designs	4-25
4.2.2	Maintainability of Fault Tolerant Designs	4-31
4.2.3	Maintainability and Testability Checklist Questions	4-34
5	FAULT TOLERANCE DESIGN AND TRADEOFF ANALYSES.	5-1
5.1	Fault Tolerance Design Methodology.	5-1
5.1.1	Baseline Design	5-1
5.1.2	Fault Avoidance Techniques	5-5
5.1.3	Development of the Fault Tolerant Design Approach	5-5
5.1.4	Fault Detection Implementation	5-6

CONTENTS (contd)

Section	Page
5.1.5 Recovery Implementation	5-6
5.1.6 R/M/T Evaluation Techniques	5-7
5.1.7 Fault Tolerant Design Methodology	
Checklist Questions	5-8
5.2 R/M/T Design Tradeoff Analyses	5-9
5.2.1 Readiness Analysis	5-9
5.2.2 Logistics Resource Analysis	5-13
5.2.3 Mission Effectiveness Analysis	5-14
5.2.4 Life-Cycle Cost (LCC) Analysis	5-14
5.2.5 R/M/T Design Tradeoff Analysis	
Checklist Questions	5-16
6 ACRONYMS	6-1
Appendix	Page
A GLOSSARY OF RELIABILITY, MAINTAINABILITY, TESTABILITY AND FAULT TOLERANCE TERMS	A-1
B REFERENCES & LIST OF GOVERNMENT DOCUMENTS. . .	B-1

LIST OF ILLUSTRATIONS

Figure	Page
1-1 Manager's Guide Overview of C ³ I Fault Tolerant Design Process	1-3
2-1 System Testability Program Flow Diagram	2-21
2-2 Verification of System Performance Characteristics	2-43
2-3 Examples of Reliability Specification of Fault Tolerant Systems	2-45
2-4 Model Requirements for Testability in a System Specification	2-49
3-1 Identification of Mission & Safety Critical Fault Tolerance Requirements.	3-3
3-2 Space Surveillance System Fault Tolerance	3-9
3-3 C ³ I Airborne Surveillance Radar Operational Concept	3-13
4-1 Elements of Fault Tolerance.	4-2
4-2 Fault Tolerance Design Options	4-9
4-3 Graceful Degradation of Antenna Receive/Transmit (R/T) Modules	4-19
5-1 Fault Tolerance Design Methodology.	5-3
5-2 Factors & Relationships Affecting Readiness & System Effectiveness	5-10
5-3 Relationship of Availability and Its Drivers MTTR & MTBM	5-12
5-4 Relationships of A_0 , Reliability, & MRT.	5-13

LIST OF TABLES

Table	Page
2-1 MIL-STD-785 Reliability Task Applications	
Guidance Matrix for Fault Tolerant Systems	2-6
2-2 MIL-STD-470 Maintainability Task Applications	
Guidance Matrix for Fault Tolerant Systems	2-13
2-3 MIL-STD-2165 Testability Task Applications	
Guidance Matrix for Fault Tolerant Systems	2-25
2-4 Typical Distribution of Software Development	
Schedule & Personnel Effort by Phase	2-33
2-5 DoD-STD-2167 Software Documentation Requirements	
Matrix	2-34
2-6 Notational Diagnostic Performance Specification	2-51
3-1 Typical Functional Criticality Prioritization	3-6
4-1 Detection Technique Characteristics	4-13
4-2 Properties of Error Detection Codes	4-13
4-3 Maintenance Concept Options	4-35
5-1 Characteristics of Current Reliability Models	5-8

1 - INTRODUCTION

Reliability, maintainability, and testability (R/M/T) are essential system attributes required to achieve the Command, Control, Communications and Intelligence program objectives of high system effectiveness and minimum life-cycle cost (LCC). A fault tolerant system design is one that has provisions to avoid failure after faults have caused errors within the system. Therefore, fault tolerant design approaches can significantly increase C³I system reliability, and are often required to meet stringent reliability requirements, assure the availability of critical C³I mission functions, and avoid potential safety hazards.

The objective of this study is to provide R/M/T design guidance for fault tolerant C³I systems. The design guidance addresses program management functions and information sources, and has been tailored for use by Air Force (AF) system planners and AF contractors. The guidelines developed as part of this study should be used to develop cost-effective requirement planning and design development programs for reliable, maintainable, and testable fault tolerant systems. Air Force and contractor program managers must provide the leadership to control the fault tolerant design process to assure that system effectiveness and LCC are not compromised. Figure 1-1 provides an overview of this Program Manager's Guide, and depicts the design process for establishing fault tolerant configurations from the program system requirements step through tradeoff analyses of alternate design approaches. As illustrated in this figure, the Guide is conveniently organized chronologically by each step of the fault tolerant design process.

Section 2 of the Guide contains an approach for planning, managing, and tailoring R/M/T programs for C³I fault tolerant system development. Tailoring is the process by which individual requirements

are evaluated to determine the extent to which they are suited for a particular system development and acquisition. The approach recommended in Section 2 evolved from an extensive review of applicable military standards governing the conduct of R/M/T and Safety programs for systems and equipment. This section also contains R/M/T program task application matrices, flow diagrams, and guidelines for the specification of fault tolerance and R/M/T requirements.

Section 3 describes the relationship between C³I program requirements and mission and safety criticality. Fault tolerance should be incorporated into a design as part of the system engineering process, since experience has shown that a hierarchical approach involving the selective application of fault tolerant design techniques is most effective. In general, fault tolerant design methodology used by system engineering personnel consists of first creating a baseline design and then systematically introducing appropriate levels of fault tolerance required to meet R/M/T requirements. A key ingredient in fault tolerant design is the application of hardware redundancy. Since added hardware increases maintenance, weight, volume, complexity, cost, and spares, it is important that fault tolerant design techniques are not used indiscriminately.

Section 4 delineates the R/M/T attributes of the various fault tolerant design options along with typical application areas. Section 5 contains a description of fault tolerant design methodology and presents the methodology used to evaluate the cost effectiveness of alternative fault tolerant design options. Appendix A contains a glossary of R/M/T and fault tolerance terms. Sources of information used in this study included DoD directives, NASA, DoD and military standards, military handbooks, open literature, and RADC technical reports on R/M/T for fault tolerance. Appendix B contains a list of references including the identification of the exact issue of military and DoD standards and NASA documents referenced in the Guide.

Within this Guide, attempts were made to identify the individual responsibilities of both AF and contractor program managers in the fault

2.0 R/M/T PROGRAM PLANNING
& MANAGEMENT

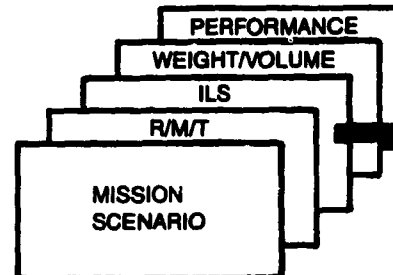


R/M/T REQMTS &
CONSTRAINTS

- MISSION SUCCESS PROB.
- LOGISTICS
- WEIGHT/VOL/POWER
- ETC

4.0

C³I PROGRAM REQMTS



DEVELOP BASELINE C³I
FUNCTIONAL
DESIGN CONFIGURATION



3.0 RELATIONSHIP OF C³I FAULT TOLERANCE TO
MISSION & SAFETY CRITICALITY

IDENTIFY CRITICAL MISSION
AND SAFETY FUNCTIONS

- MISSION CRITICALITY
ANALYSIS
- SAFETY ASSESSMENT

R87-5011-500

R87-3537-001 (T)

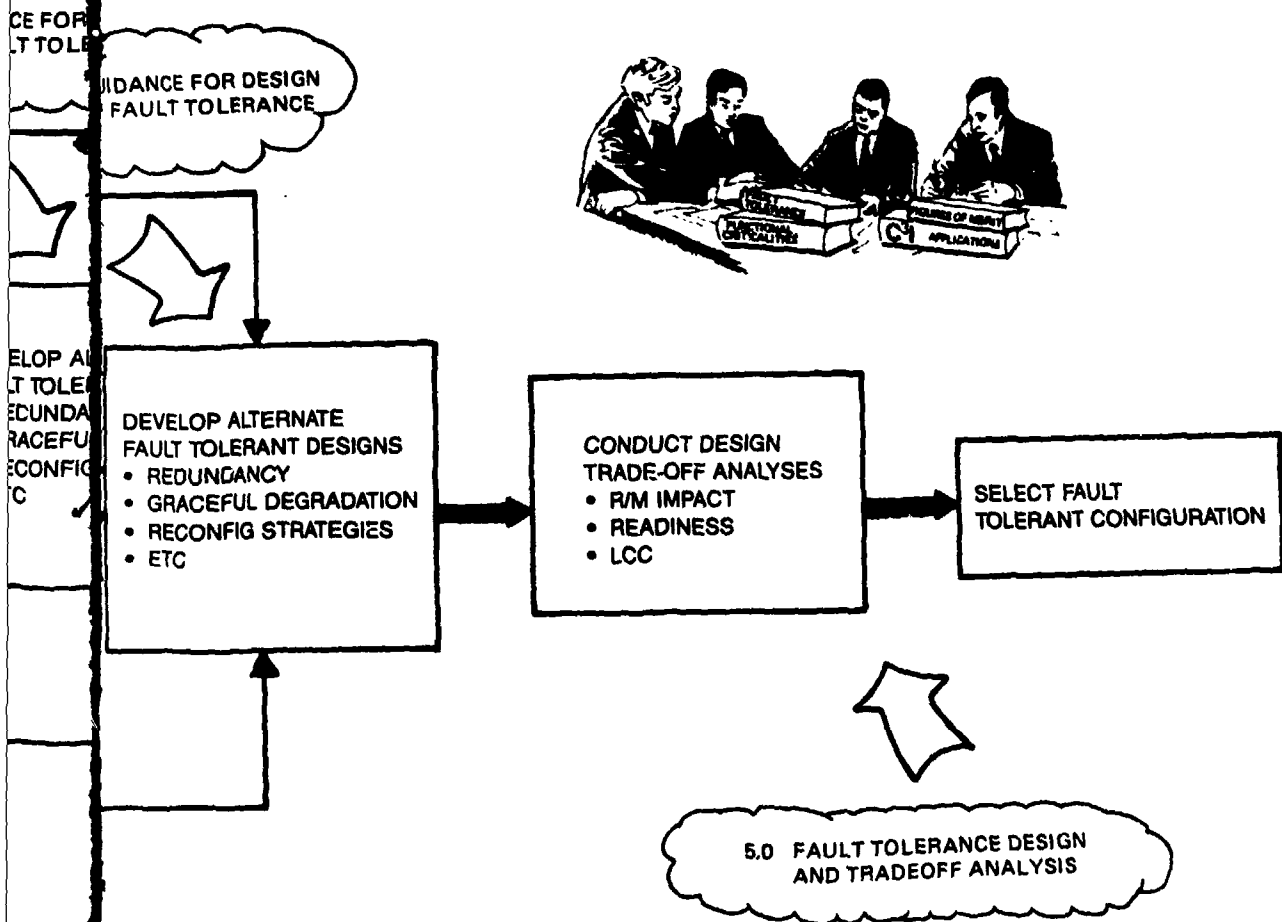


Figure 1-1. Manager's Guide Overview of C³
Fault Tolerant Design Process.

tolerance design process. The AF program managers are responsible for the establishment of system program requirements and the approval of design configurations. The prime and systems integration contractors are responsible for the development and optimization of design configurations that satisfy the system requirements. To assure a cost-effective program, both the AF and the contractor must work together to formulate realistic system requirements and conduct design tradeoff analyses. Therefore, all the material presented herein should be of interest to both AF and contractor program managers.

Program managers should address the checklist questions provided at the end of each section. Unless specifically noted, the checklist questions apply both to AF and contractor program managers. These questions are particularly applicable at the System Requirements Review (SRR), Preliminary Design Review (PDR), and Critical Design Review (CDR) to supplement the R&M evaluation criteria listed in MIL-STD-1521, *Technical Reviews and Audits for Systems, Equipment and Computer Software*. Questions primarily addressed to the Procuring Activity are followed by a (PA). Those addressed to integrating or prime contractors are followed by a (C).

2 - R/M/T PROGRAM PLANNING AND MANAGEMENT

This section contains an approach to tailoring R/M/T programs for C³I fault tolerant systems development. Task application matrices, flow diagrams and areas of special emphasis are provided to assist AF program managers in R/M/T program planning and management. Management guidelines are provided for the specification of fault tolerance and R/M/T requirements, for software program management and for Reliability and Maintainability (R&M) warranties.

2.1 SYSTEM TAILORED APPROACH

The R/M/T tasks and associated application matrices (delineated in MIL-STD-785B, MIL-STD-470A and MIL-STD-2165, respectively) are applicable to the development programs of fault tolerant systems. In general, these military standards adequately describe the R/M/T tasks recommended for implementation when developing fault tolerant systems.

However, there are some task guidelines and tailoring that an AF program manager should consider when developing a Statement of Work (SOW) for a fault tolerant system. These guidelines are described in paras. 2.1.1, 2.1.2, and 2.1.3 of this Guide along with descriptions of other tasks that are important in the formulation of overall R/M/T programs.

R/M/T task tailoring depends upon the performance requirement levels that must be achieved and the expected extent of new design and development involved. For example, a new strategic C³I system would require a more extensive application of R/M/T tasks than that of an evolutionary C³I system design approach which utilizes existing and qualified equipment/subsystems. All procurements require analysis to specify

R/M/T levels. If mission criticality requirements are found to be low, it may be possible to reduce acquisition costs by procuring commercial off-the-shelf (COTS) equipment. In general, the procurement of COTS equipment requires effort to select items with "as is" suitability and demonstrated acceptability to meet program needs. (Refer to MIL-HDBK-338, para. 12.7.) Hence, the emphasis in procurement of COTS equipment is in selection, not specification. For these reasons, a reduced set of R/M/T tasks may be appropriate and cost-effective for fault tolerant C³I system programs that incorporate extensive use of COTS equipment.

An Air Force program manager should consider the following subset of R/M/T tasks when developing Statements of Work:

- Program plans - Since the program plan identifies and ties together all program management tasks deemed necessary to support the economical achievement of overall R/M/T program objectives, the plan is a necessary ingredient in any system development/acquisition
- Allocation of specification requirements - The allocation process is necessary since it transforms overall system R/M/T requirements into manageable lower level requirements for subsystems and equipments
- Design criteria - Provide standards for design compliance and help shape fault tolerant system architectures with the minimum of added redundancy and complexity
- Trade studies - Tradeoffs between alternate fault tolerant configurations which are capable of meeting system R/M/T requirements are mandatory to assure that the most cost-effective design approach is utilized
- Subcontractor and supplier control - The primary contractor's understanding and control of a subcontractor's R/M/T program is fundamental to meeting overall program goals

- **Thermal design analysis** - Reduction in the operating temperature of components is a primary method of improving reliability, and is often as important as circuit design in obtaining the necessary performance characteristics from electronic equipment
- **Predictions (including Built-In Test (BIT)/preventive maintenance/diagnostic capability)** - Predictions combine lower level R/M/T data to indicate equipment parameters at successively higher levels from subassemblies through subsystems to the system. Predictions that fall short of requirements at any level may signal the need for management and technical action
- **Effects of functional testing, storage, handling, packaging, transportation, and maintenance** - The results of analyses in these areas are needed to support long-term failure rate predictions, design tradeoffs, definition of allowable test exposures, packaging, handling and storage requirements, and refurbishment plans
- **Test/verification planning** - R/M/T test and verification procedures are required to: (1) disclose deficiencies in the system design, material, and workmanship; (2) provide R/M/T data for estimates of operational readiness, mission success, maintenance manpower, and logistics support costs; and (3) determine compliance with quantitative R/M/T requirements
- **Environmental Stress Screening (ESS)** - ESS procedures are required so that failures due to weak parts, workmanship defects, and other non-conformance anomalies can be identified and removed from the equipment, or so appropriate redesign measures may be taken
- **Failure Reporting, Analysis and Corrective Action System (FRACAS)** - A well organized system for collecting, analyses/review, dissemination, and close-out of failure reports is essential to the workings of an R&M program, and can provide management visibility into problem areas

- **Participation in design reviews (PDR, CDR, etc.)** - Review of R/M/T program status at specified points is necessary to assure that the program is proceeding in accordance with contractual milestones and that system R/M/T requirements will be achieved
- **Operational assessment** - Operational systems should be continually assessed to assure that they are performing in accordance with predictions and to identify areas where improvements can be incorporated to minimize degradation, improve R/M/T, and reduce the LCC
- **Testability program and requirements** - To assure development of the fault detection and fault isolation capability that is necessary to support system reconfiguration, maintenance diagnostics, and achievement of overall program R&M requirements, a testability program should be conducted as part of any fault tolerant system development/acquisition
- **Built-In Test analysis** - The analysis of BIT features and BIT equipment designs that will be used to detect and isolate faults, support redundancy management, and system reconfiguration are necessary to assure that the desired fault tolerance performance levels are achieved.

In addition to the task application matrices contained in MIL-STD-785, -470 and -2165, R&M system tailoring guidance (based on R&M requirement levels and design maturity) is also contained in MIL-HDBK-338, *Electronic Reliability Design Handbook*. For these military standards, additional specific application guidelines to fault tolerant system development efforts are provided in the following subsections.

2.1.1 Reliability Program Tailoring

Before selecting, tailoring and integrating reliability tasks for a C³I development program, the AF program manager should refer to the pertinent application guidance contained in Appendix A of MIL-STD-785. Some

reliability tasks applicable to fault tolerant system developments require additional emphasis with regard to advancing their implementation schedule and require a higher level of effort. The MIL-STD-785 task application matrix, modified for fault tolerant system developments, is shown in Table 2-1. Reliability tasks that require additional emphasis and tailoring in both the Statement of Work (SOW) and associated CDRLs for fault tolerant system developments are discussed in the paragraphs that follow. In addition, a number of other reliability tasks, which are implemented in the same way for both fault tolerant and non-fault tolerant systems, have been included due to their importance in the formulation of the overall reliability program.

- *Task 101, Reliability Program Plan* - The procedures and content for this task are the same for fault tolerant and non-fault tolerant systems. However, a write-up on the task description has been provided since this task is deemed to be "generally applicable" during all program phases for fault tolerant system development. The plan provides management visibility for proper monitoring, control and coordination between interrelated design and support activities. The Full-Scale Engineering Development phase SOW should require the contractor to develop specific fault tolerance questions for inclusion in the design review checklist. It is also recommended that this SOW include a requirement for the development of a Fault Tolerance Test Plan which details plans for evaluating and demonstrating how well the design meets fault tolerance requirements, especially with regard to fault protection coverage and fault recovery times.
- *Task 104, Failure Reporting, Analysis and Corrective Action System (FRACAS)* - The stringent reliability requirements attendant to fault tolerant systems require the early elimination of failure causes since this process is a major contributor to relia-

TABLE 2-1. MIL-STD-785 Reliability Task Applications Guidance Matrix for Fault Tolerant Systems.

TASK	TITLE	TASK TYPE	PROGRAM PHASE			
			CONCEPT	VALID	PROD	PROD
101	RELIABILITY PROGRAM PLAN	MGT	■	■	G	G
102	MONITOR/CONTROL OF SUBCONTRACTORS & SUPPLIERS	MGT	S	S	G	G
103	PROGRAM REVIEWS	MGT	S	S(2)	G(2)	G(2)
104	FAILURE REPORTING, ANALYSIS & CORRECTIVE ACTION SYSTEM (FRACAS)	ENGRG	NA	S	G	G
105	FAILURE REVIEW BOARD (FRB)	MGT	NA	S(2)	G	G
201	RELIABILITY MODELING	ENGRG	■	■	G(2)	GC(2)
202	RELIABILITY ALLOCATIONS	ACCT	■	G	G	GC
203	RELIABILITY PREDICTIONS	ACCT	■	■	G(2)	GC(2)
204	FAILURE MODES, EFFECTS, & CRITICALITY ANALYSIS (FMECA)	ENGRG	■	■	G(1)(2)	GC(1)(2)
205	SNEAK CIRCUIT ANALYSIS (SCA)	ENGRG	NA	NA	G(1)	GC(1)
206	ELECTRONIC PARTS/CIRCUITS TOLERANCE ANALYSIS	ENGRG	NA	NA	G	GC
207	PARTS PROGRAM	ENGRG	S	S(2)	G(2)	G(2)
208	RELIABILITY CRITICAL ITEMS	MGT	S(1)	■	G	G
209	EFFECTS OF FUNCTIONAL TESTING, STORAGE HANDLING, PACKAGING, TRANSPORTATION & MAINTENANCE	ENGRG	NA	S(1)	G	GC
301	ENVIRONMENTAL STRESS SCREENING (ESS)	ENGRG	NA	S	G	G
302	RELIABILITY DEVELOPMENT/GROWTH TESTING	ENGRG	NA	S(2)	G(2)	NA
303	RELIABILITY QUALIFICATION TEST (RQT) PROGRAM	ACCT	NA	S(2)	G(2)	G(2)
304	PRODUCTION RELIABILITY ACCEPTANCE TEST (PLAT) PROGRAM	ACCT	NA	NA	S	G(2)

NOTE: PROGRAM PHASE APPLICABILITY CHANGES FROM TABLE A-1 OF MIL-STD-785 ARE SHOWN WITH ■

CODE DEFINITIONS

TASK TYPE

ACCT - RELIABILITY ACCOUNTING

ENGRG - RELIABILITY ENGINEERING

MGT - MANAGEMENT

PROGRAM PHASE

S - SELECTIVELY APPLICABLE

G - GENERALLY APPLICABLE

GC - GENERALLY APPLICABLE TO DESIGN CHANGES ONLY

NA - NOT APPLICABLE

(1) - REQUIRES CONSIDERABLE INTERPRETATION OF INTENT TO BE COST EFFECTIVE

(2) - MIL-STD-785 IS NOT THE PRIMARY IMPLEMENTATION REQUIREMENT. OTHER MIL-STDs OR STATEMENT OF WORK REQUIREMENTS MUST BE INCLUDED TO DEFINE THE REQUIREMENTS.

R87-3537-002(T)

bility growth and attainment of acceptable field reliability. During Full-Scale Engineering Development, the FRACAS should be required to document hardware anomalies, software errors and masked faults. This enhances the ability to develop corrective action and monitor the reliability growth of the system. The procedure for implementing the FRACAS on fault tolerant systems is the same as that used on non-fault tolerant systems.

- *Task 201, Reliability Modeling* - The development of reliability models is mandatory for fault tolerant system development since the evaluation of these models is an integral part of trade study activity aimed at developing and selecting the lowest LCC configuration capable of meeting R/M/T requirements. This task is "generally applicable" to all program phases since careful review of even the early models can reveal states or conditions where management action may be required. The mission success probability model should be developed to the extent that information becomes available concerning the fault protection/redundancy configuration(s), even though numerical input data may not be available. Single point failure states, which can cause premature mission loss or unacceptable safety hazards, can be readily identified and targeted for additional design consideration. The methodology and procedures used for fault tolerant systems reliability modeling differ from that of other systems in that analysis of fault tolerant systems generally deals with the much more complex models required to evaluate reconfigurable and resource sharing configurations.

Mission reliability models for evaluating conventional series-parallel equipment configurations should be based on the techniques described in Methods 1001 thru 1004 of MIL-STD-756. Mission reliability modeling of systems employing extensive hardware redundancy and complex fault management, recovery and

reconfiguration techniques often requires sophisticated evaluation tools that are typically based on Markov analysis techniques and Monte Carlo simulation methods. In addition, these tools and models typically consider the following situations:

- Redundancies present
- Permanent faults
- Transient or intermittent faults
- Effects of failure modes
- Propagating sequences of faults
- Mission load changes
- System response to failure if fault protection coverage (consisting of detection, isolation, recovery or reconfiguration) is less than perfect.

Some currently existing computerized models used for the reliability assessment of these complex fault tolerant systems are ARIES, CARE III, HARP, and SURE (see para. 5.1.6).

- *Task 202, Reliability Allocations* - For fault tolerant system developments, this task should be started during the Concept Exploration phase in conjunction with the establishment of system level requirements. Early management visibility of subsystem allocations may highlight the reasonableness of these system level requirements and, if warranted, cause their reassessment. In later program phases, if some of the subsystem and lower level allocations appear to be unreasonably difficult to achieve, then the analysis becomes the basis for performing fault tolerant design and redundancy tradeoffs among the subsystems. The subsequent reallocation should provide lower equipment level reliability requirements/specifications which can reasonably be achieved. Both SOW and CDRL requirements for reliability allocations and predictions also require the performance of task 201 for consistency and traceability.

- **Task 203, Reliability Predictions** - This task is deemed to be "generally applicable" during all phases of fault tolerant system development since, when these predictions are coupled with the models of task 201, the early mission completion success probability predictions will identify those subsystems that contribute a high percentage to the total probability of mission failure. This process will identify those areas requiring increased fault tolerance and where management action may be directed to yield the highest payoff. Early review of reliability predictions at the lowest equipment levels will identify parts or components which may have inadequate margins between the parts strength and the expected applied stress. In addition, the earlier the review is performed, the greater the range of acceptable options for improving equipment reliability. Whenever predictions fall short of allocated reliability requirements, alternatives such as the following should be considered:
 - Identify suitable higher reliability substitutes
 - Reapportion reliability allocations
 - Redesign using higher reliability parts or more fault tolerant designs
 - Decrease the severity of environments or other operational stress factors.

Some alternatives are more feasible and acceptable than others at given points in development, but all are easier and less expensive to accomplish earlier than later. Equipment level reliability predictions for fault tolerant systems must take into account redundancies present in lower tier hardware elements.

- **Task 204, Failure Mode, Effects and Criticality Analysis (FMECA)**
 - This task is "generally applicable" during all phases of fault tolerant system development. In particular, imposition of this

task is recommended at the system level during the Concept Exploration phase and at lower levels, as applicable, during the Demonstration/Validation phase. The FMECA results should be used to confirm the validity of the reliability model (task 201) for compliance with qualitative fault tolerance criteria (eg., fail operational/fail-safe requirements, etc.), and for computing reliability estimates of subsystems or functional equipment groupings, particularly where redundancy or fault protection is present. The SOW and CDRL must also identify the equipment level at which the FMECA is conducted, taking into consideration any specification requirements relating to the system level at which faults will or will not be tolerated. During the Full-Scale Engineering Development phase, the FMECA must also be conducted on highly mission critical systems with emphasis on relevant *fault classes* such as transient, intermittent, permanent, latent, common cause and catastrophic failures. The procedures for implementing FMECAs on fault tolerant systems are quite similar to those used on non-fault tolerant systems. However, where multiple layers of redundancy or reconfiguration capability in response to failures is provided, the FMECA activity must include a review of testability features to assure that adequate fault detection/fault isolation capability exists to preclude fault propagation and support system reconfiguration.

- *Task 208, Reliability Critical Items* - For fault tolerant system development, it is recommended that this task be initiated during the Demonstration/Validation phase to the extent that analysis (e.g. FMECA) of system configurations has identified items whose failure can significantly affect system safety, mission success, availability or total maintenance/logistics support cost. Reliability critical items, once identified as a part of the selected configurations, should be retained and closed-out in subsequent

program phases. Reliability critical items which cannot be eliminated by design are the prime candidates for additional analysis, growth testing, reliability qualification testing, reliability stress analyses, and other techniques to reduce the systems reliability, availability or LCC risk. It is advisable to request the prime contractor to examine the list of reliability critical items and make appropriate recommendations for additions and deletions with supporting rationale.

- ***Task 303. Reliability Qualification Test (RQT) Program -***

Reliability qualification testing provides a reasonable assurance that a subsystems/systems minimum acceptable reliability requirements have been met before committing to production. Normally, RQTs of non-redundant items utilize test plans to statistically verify the item's specified minimum acceptable mean-time-between-failure (MTBF). A mission-time-between-critical-failure (MTBCF) requirement contained in the System Specification of a fault tolerant system should be verified by analysis or test. It is recommended that AF program managers consider selectively supplementing MTBF RQT's for fault tolerant system equipment by requiring verification of MTBCF requirements by demonstration test. This recommendation applies to highly mission/safety critical subsystems/systems which contain redundant equipments with low MTBFs. It also applies when the complexity of the system's fault tolerant protection mechanism may limit confidence in analytical approaches to MTBCF verification. However, the presence of high MTBCF values or low volume production may make it impossible to demonstrate the MTBCF with statistical confidence. In these cases, the program manager should require that the MTBCF be verified by rigorous analysis that includes, as appropriate, the use of a proven reliability model (see para. 5.1.6) and/or computer simulation techniques. MIL-STD-781, *Reliability*

Design Qualification and Production Acceptance Tests: - *Exponential Distribution* cannot be used to accurately assess the decision risks related to the reliability demonstration of fault tolerant/redundant systems, since the distribution of times-to-failure of such systems do not follow an exponential function. However, a Monte Carlo simulation program is capable of solving this problem and:

- Evaluating and defining the producer and consumer risks for various system MTBCF values
- Offering optional selection of sequential or fixed length test plans
- Allowing evaluation of systems which operate under either deferred or periodic maintenance policies.

A Monte Carlo simulation program for MTBCF demonstration tests has been developed and is described in *Reliability Demonstration Technique for Fault Tolerant Systems* (Reference 1).

Additional reliability tasks for the development of fault tolerant systems include performing those trade studies and analyses required to define a reliable and supportable system architecture that is also cost effective. It is important that the selected reliability tasks be coordinated with associated Maintainability, Testability, Logistics Support and System Safety tasks and analyses.

2.1.2 Maintainability Program Tailoring

As described in MIL-STD-470A, Appendix A, Section 30, cost-effective task selection and tailoring can materially aid in attaining program maintainability requirements. Some maintainability tasks, applicable to fault tolerant system development, require additional emphasis with regard to advancing their implementation schedule and requiring a higher level of effort. The MIL-STD-470 task application matrix, modified for fault tolerant system developments, is shown in Table 2-2.

TABLE 2-2. MIL-STD-470 Maintainability Task Applications Guidance Matrix for Fault Tolerant Systems.

TASK	TITLE	TASK TYPE	PROGRAM PHASE				
			CONCEPT	VALID	FSD	PROD	OPER SYSTEM DEV (MODS)
101	MAINTAINABILITY PROGRAM PLAN	MGT	■	G(3)	G	G(3)(1)	■
102	MONITOR/CONTROL OF SUB-CONTRACTORS AND VENDORS	MGT	N/A	S	G	G	S
103	PROGRAM REVIEWS	MGT	S	G(3)	G	G	S
104	DATA COLLECTION, ANALYSIS AND CORRECTIVE ACTION SYSTEM	ENG	N/A	S	G	G	■
201	MAINTAINABILITY MODELING	ENG	S	S(4)	G	C	■
202	MAINTAINABILITY ALLOCATIONS	ACC	■	■	■	C	■
203	MAINTAINABILITY PREDICTIONS	ACC	■	■	G(2)	C	■
204	FAILURE MODES AND EFFECTS ANALYSIS (FMEA) MAINTAINABILITY INFORMATION	ENG	N/A	S(2) (3)(4)	G(1) (2)	C(1) (2)	■
205	MAINTAINABILITY ANALYSIS	ENG	S(3)	G(3)	■	■	■
206	MAINTAINABILITY DESIGN CRITERIA	ENG	■	S(3)	G	C	■
207	PREPARATION OF INPUTS TO DETAILED MAINTENANCE PLAN AND LOGISTICS SUPPORT ANALYSIS (LSA)	ACC	N/A	S(2) (3)	G(2)	C(2)	■
301	MAINTAINABILITY DEMONSTRATION (MD)	ACC	N/A	S(2)	G(2)	C(2)	S(2)

NOTE: PROGRAM PHASE APPLICABILITY CHANGES FROM TABLE A-1 OF MIL-STD-470 ARE SHOWN WITH ■

CODE DEFINITIONS

TASK TYPE

ACC - MAINTAINABILITY ACCOUNTING
ENG - MAINTAINABILITY ENGINEERING
MGT - MANAGEMENT

PROGRAM PHASE

S - SELECTIVELY APPLICABLE
G - GENERALLY APPLICABLE
C - GENERALLY APPLICABLE TO DESIGN CHANGES ONLY
N/A - NOT APPLICABLE

- (1) REQUIRES CONSIDERABLE INTERPRETATION OF INTENT TO BE COST EFFECTIVE.
- (2) MIL-STD-470 IS NOT THE PRIMARY IMPLEMENTATION DOCUMENT. OTHER MIL-STDs OR STATEMENT OF WORK REQUIREMENTS MUST BE INCLUDED TO DEFINE OR RESCIND THE REQUIREMENTS. FOR EXAMPLE MIL-STD-471 MUST BE IMPOSED TO DESCRIBE MAINTAINABILITY DEMONSTRATION DETAILS AND METHODS.
- (3) APPROPRIATE FOR THOSE TASK ELEMENTS SUITABLE TO DEFINITION DURING PHASE.
- (4) DEPENDS ON PHYSICAL COMPLEXITY OF THE SYSTEM UNIT BEING PROCURED, ITS PACKAGING AND ITS OVERALL MAINTENANCE POLICY.

R67-3537-003(T)

Systems managers incorporating a high degree of fault tolerance in their designs should use this matrix with emphasis on early program phases, particularly the Concept Exploration and the Demonstration/Validation phases. Effective and feasible concepts for Maintainability, Diagnostics and Maintenance must be developed and applied as early as possible to insure that major alternatives can be examined for overall impact on performance and LCC before system design is "cast in concrete." Earlier corrective actions can thereby be initiated and maintainability inputs can be provided for evaluating the impact on mission reliability, readiness, as well as LCC. Crucial issues such as mission-related and large cost-impact items are, therefore, addressed earlier in a more comfortable and realistic time frame. For example, the proposed addition of redundant subsystem/equipment/modules may appear to improve overall mission reliability with a minor penalty of additional technical, operational or testability complexity. Without the timely maintainability evaluation of the critical design changes for this added redundancy, the diagnostics and accessibility of an otherwise easy access point could be compromised and result in a severe impact to the item's mean-time-to-repair capability. Maintainability tasks that require additional emphasis and tailoring in both the SOW and associated CDRLs for fault tolerant system developments are discussed in the paragraphs that follow. In addition, a number of other maintainability tasks, which are implemented in the same way for both fault tolerant and non-fault tolerant systems, have been included due to their importance in the formulation of the overall maintainability program.

- *Task 101, Maintainability Program Plan* - The development of a maintainability program plan for fault tolerant systems should be considered as "generally applicable" for all program phases and all system modifications. The plan is needed early in the development cycle to define the early concepts necessary to guide the maintainability program during subsequent program phases. The primary objectives of a maintainability program are to ensure

design adherence to specified maintainability parameters in an environment of maintenance, support, and lower LCC constraints. Diagnostics, for instance, provide multiple capabilities for redundancy management, fault tolerance, on-line performance monitoring, and basic maintenance fault localization functions. Identification and analysis of risks play a key role due to the high level of uncertainty that is present early in a system's life cycle. The maintainability program plan should identify all maintainability analyses to be performed. These analyses are necessary to establish and identify the risks involved in levels of repair, false alarm rates, proportion of faults detectable, levels of isolation, and development of external test systems. The maintainability program plan should provide management a description of how the contractor intends to satisfy mission maintainability requirements. This task is implemented in the same way for both fault tolerant and non-fault tolerant systems. It should be noted that the maintainability program plan may be submitted as an integrated plan including reliability and testability.

- *Task 104, Data Collection, Analysis, and Corrective Action System* - This task is established to aid design, identify corrective action tasks and evaluate test results. The data collection system should be defined as early as possible, but not later than the Demonstration/Validation phase and should be considered as "generally applicable" for all system modifications. The data collection system used during the maintainability demonstration should receive preliminary planning during the Demonstration/Validation phase and should become firm in the maintainability demonstration plan prior to testing. The data collection system should be used as a means for identifying maintainability design problems and errors, and for initiating corrective actions. These corrective actions can take the form of modifications and

changes to equipment maintenance procedures and fault detection and isolation features (hardware and software) to improve the faults detectable, fraction of faults isolatable, and reduce false alarm rates, maintenance induced faults, system outages and excessive corrective or preventive maintenance times.

- *Task 201, Maintainability Modeling* - During the Concept Definition and Demonstration/Validation phases, various fault tolerant system design and support alternatives may be evaluated through the use of models. The models previously developed during the Full-Scale Development phase, should be updated and used to measure the progress achieved versus the specified requirements and goals. These models should also be used to evaluate the maintainability impact of design changes. The models may also be utilized to determine the impacts of changes in fault detection probability, fraction of isolatable failures, and frequency of failures. For fault tolerant systems designed for an on-line maintenance concept, the maintainability modeling task must consider the effect of on-line maintenance on system performance and the ability of the system to meet overall R&M requirements.
- *Task 202, Maintainability Allocations* - The maintainability allocation process is the same for both fault tolerant and non-fault tolerant systems. However, since stringent availability requirements are usually imposed on fault tolerant systems, it is important that overall system maintainability objectives be translated into maintainability requirements for system components. Maintainability is a key factor affecting availability (see para. 5.2.1); accordingly, maintainability allocations should be conducted on system elements suitable to definition during the early program phases when the most flexibility in tradeoffs and redef-

initiation exists. Starting early also allows time to establish lower level maintainability and system level diagnostic requirements that can be allocated to subsystems, and diagnostic requirements that can be allocated to assemblies. Also, the maintainability requirements must be frozen at some point to provide a baseline for the designer. Fault detection and fault isolation probabilities to a given level must be defined.

- *Task 203, Maintainability Predictions* - The maintainability prediction process is the same for fault tolerant and non-fault tolerant systems. This task should be selectively applied during the Concept Exploration phase to evaluate and tradeoff various fault tolerant system design configurations. However, during the Demonstration/Validation and Full-Scale Development phases, maintainability predictions should be used to determine the degree of compliance to specification requirements. Up to date predictions provide engineers and management with essential information on maintainability program progress; in addition, they are important elements in the program decision making process. Since a limited quantity of specific design data may be available during the Demonstration/ Validation phase, maintainability predictions must be based largely on experience with predecessor (similar) systems and on reliable/proven prediction techniques. During the Full-Scale Development phase, maintainability predictions can be used to determine the inherent maintainability characteristics of the proposed system, the effects of proposed changes on maintainability, and the optimum tradeoff of equipment characteristics. Predictions made during this phase are generally more accurate than those made in earlier phases, since more specific system information is available.

- *Task 204, Failure Mode and Effects Analysis (FMEA)* - A FMEA is used to identify critical failure modes and checks the diagnostic capability for detecting and isolating each of these modes. Specifically, this capability relates to such activities as the determination and design of indices of failure, placement and nature of test points, development of troubleshooting schemes, and the establishment of design characteristics and criteria for fault detection and isolation at all equipment levels. The effectiveness of this fault detection and isolation capability becomes a critical driver for maintainability design at organizational, intermediate, and depot maintenance levels. Potential design weaknesses which seriously impact safety, reliability, or maintainability are identified through the proper use of the FMEA, BIT/self-test (ST), and preventive/corrective maintenance analyses. Top-level FMEA activity should be initiated during the Concept Exploration phase where only more obvious failure modes may be identified since design definition is limited. As greater design and mission definition becomes available during Demonstration/Validation and Full-Scale Development phases, the analysis should be expanded to successively more detailed levels (ie., system, subsystem, and equipment levels) and ultimately to the piece part level if warranted based on mission criticality.

- *Task 205, Maintainability Analysis* - The tradeoff process required to pick the fault tolerant design best suited to meet system R/M/T requirements and program LCC constraints requires a maintainability analysis. In general, this task has four main purposes: (1) to establish design criteria that will provide the desired system features; (2) to allow for design decisions to be made through the evaluation of alternatives and through the use of tradeoff studies; (3) to contribute toward the development of maintenance, repair, and servicing policies best suited to the

system; and (4) to verify that the design complies with maintainability design requirements.

- **Task 206, Maintainability Design Criteria** - For the stringent maintainability requirements typically imposed on fault tolerant systems to be tailored into practical and effective hardware designs, it is recommended that a broad spectrum of maintainability design criteria be defined and employed. Although the task procedures are the same as those used for non-fault tolerant systems, this task should be considered as "selectively applicable" during the Concept Exploration phase and "generally applicable" for all design changes.
- **Task 301, Maintainability Demonstration** - Planning for this task should start no later than the beginning of the Full-Scale Development phase. Maintainability demonstration is the process in which a test is conducted to show whether or not an item possesses satisfactory maintainability characteristics. The specific approach used can range from limited controlled tests to an extensive controlled field test of the product. The test methods and requirements for the formal maintainability demonstration should be established in accordance with MIL-STD-471 and introduced in the Request for Proposal (RFP). The SOW should specify details concerning the required nature, conduct and substance of the test(s) to be performed.

The Contracting Activity should determine the need, type and scope of the formal maintainability demonstration test. The decision should be based on mission requirements, costs of tests, and type of equipment being developed. A maintainability demonstration does not guarantee achievement of the required maintainability requirements. However, it will focus attention on the item's marginal performance, particularly when the demonstration

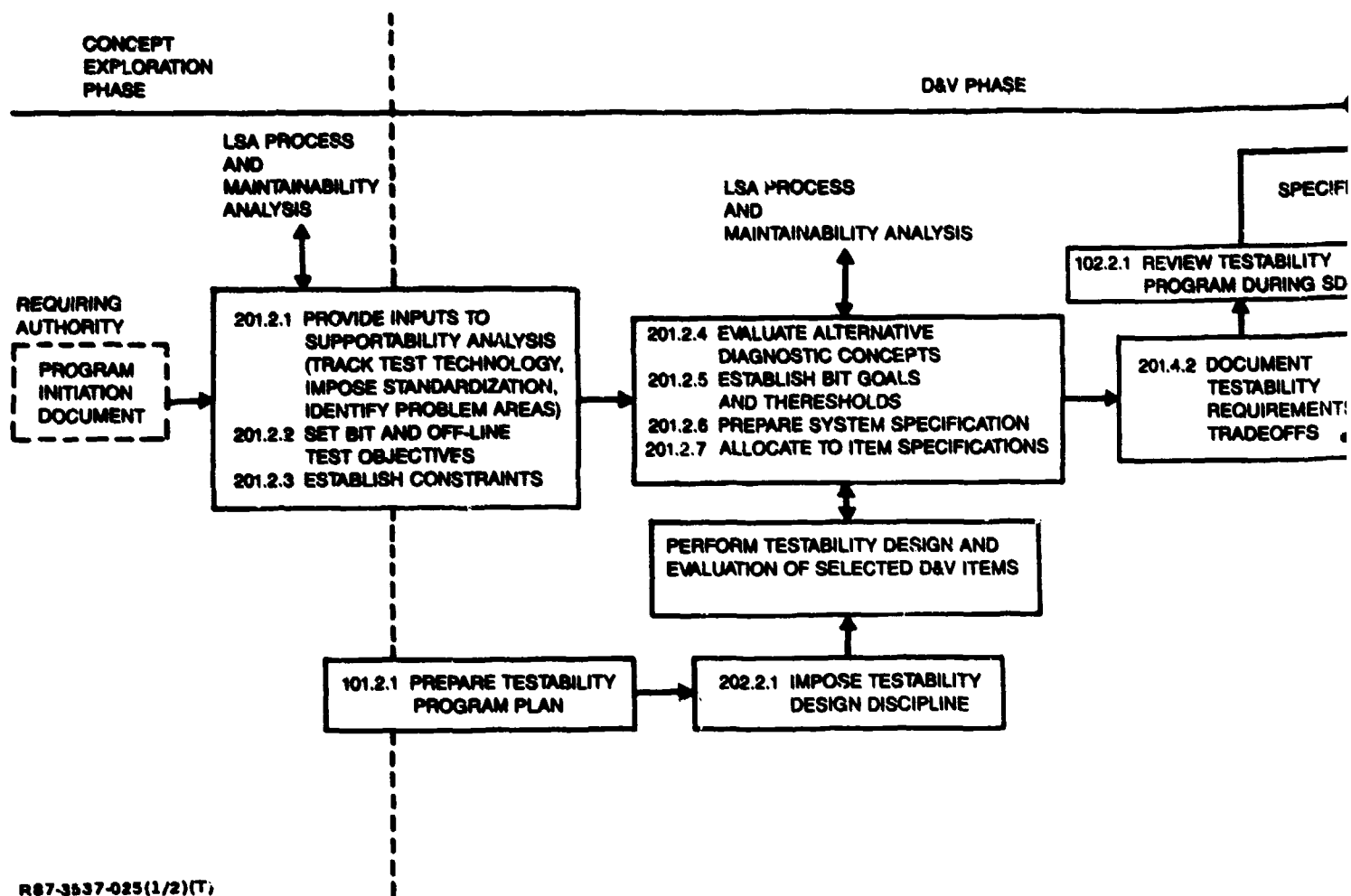
is structured properly to evaluate the maintainability design features. In particular, if fault tolerant system requirements dictate that system operation continue while a redundant system is being maintained, the planned maintainability demonstration should test this capability. The Contracting Activity should also supply information that is based on operational and deployment constraints. This provides the basis for defining realistic test procedures. As a minimum this information should include the maintenance philosophy, descriptions of the maintenance environments, the modes of operation for the test, and the levels of maintenance to be demonstrated.

For fault tolerant systems, the above stated maintainability tasks should be coordinated with associated Reliability, Testability, Human Factors, Logistic Support, and System Safety tasks and analyses.

2.1.3 Testability/Diagnostic Program Tailoring

Before selecting, tailoring, and integrating testability/diagnostic tasks into a C³I system program, the AF program manager should review the testability program application guidance included in Appendix A of MIL-STD-2165 and in particular, the System Flow Diagram illustrated in Figure 1 therein. For convenience, the System Testability Program Flow Diagram is reproduced as Fig. 2-1 herein. The MIL-STD-2165 task application matrix, modified for fault tolerant system developments, is shown in Table 2-3. Both Fig. 2-1 and Table 2-3 are relevant to most applications, including systems that incorporate a high degree of fault tolerance.

The testability design process must take into account both spatial and temporal considerations for fault detection. In particular, the failure detection approach selection must be based upon the requirement for maximum acceptable failure latency. Continuous failure detection techniques should be used to monitor those functions which are mission critical and/or affect safety and where protection must be provided



R87-3537-025(1/2)(T)

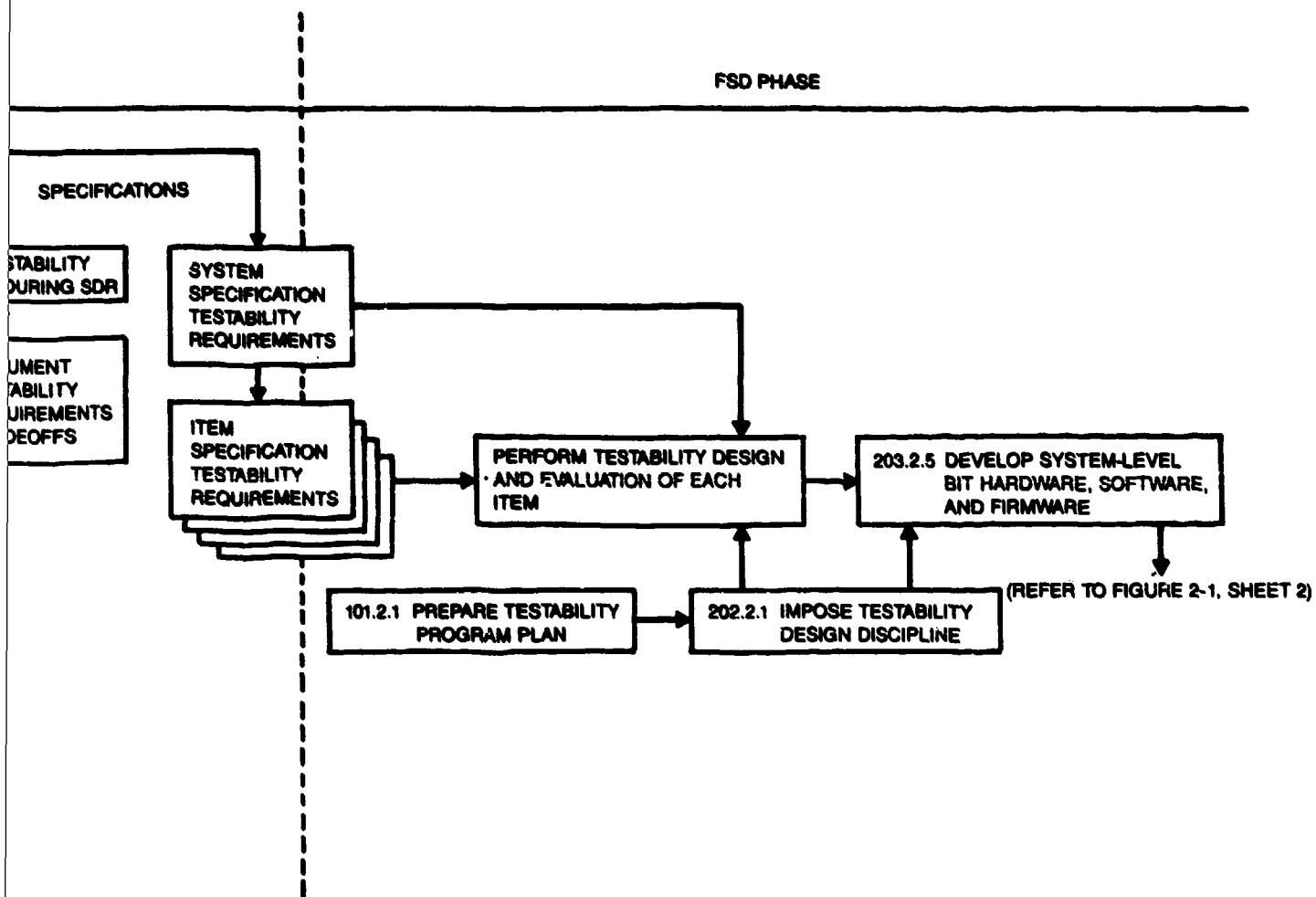
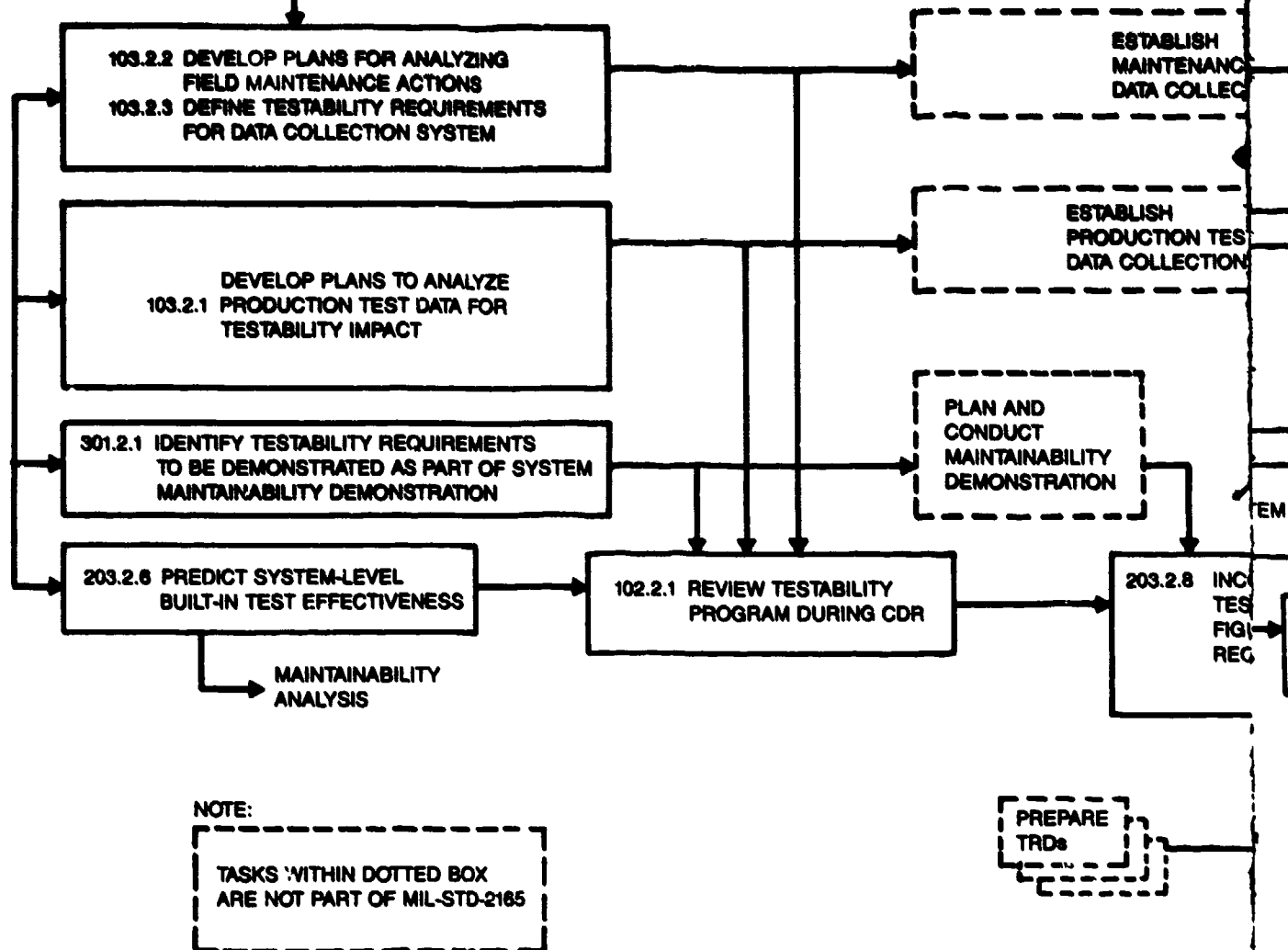


Figure 2-1. System Testability Program Flow Diagram.
(Sheet 1 of 2)

FSD PHASE

(CONTINUED FROM FIG. 2-1. SHEET 1)



R87-3537-025(2/2)(T)

Figure 2-1.

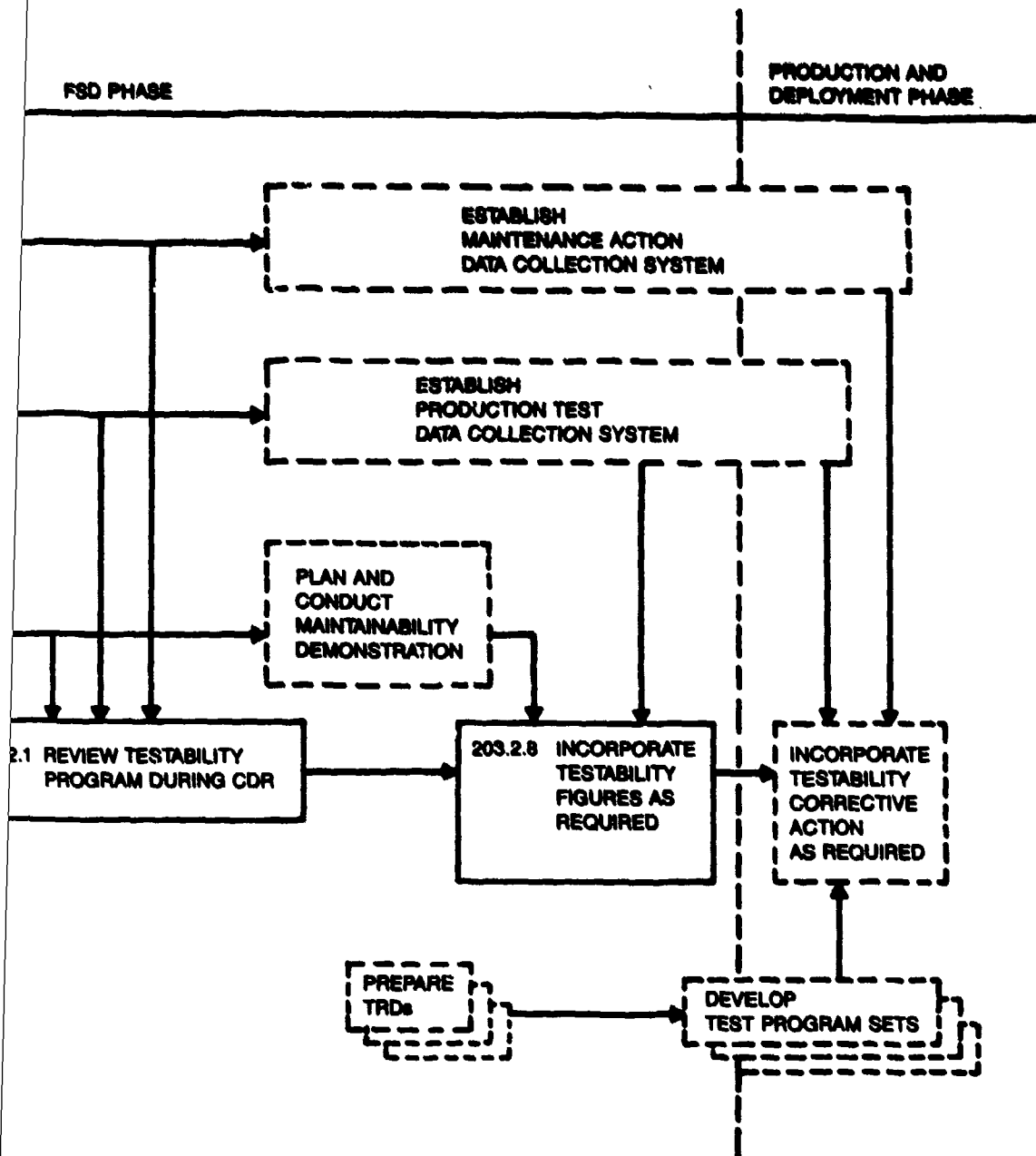


Figure 2-1. System Testability Program Flow Diagram.
 (Sheet 2 of 2)

**TABLE 2-3. MIL-STD-2165 Testability Task Applications Guidance Matrix
for Fault Tolerant Systems.**

TASK	TITLE	PROGRAM PHASE			
		CONCEPT	D & V	FSD	PROD
101	TESTABILITY PROGRAM PLANNING	■	G	G	NA
102	TESTABILITY REVIEWS	G(1)	G	G	S
103	TESTABILITY DATA COLLECTION AND ANALYSIS PLANNING	NA	S	G	G
201	TESTABILITY REQUIREMENTS	G(1)	G	G	NA
202	TESTABILITY PRELIMINARY DESIGN AND ANALYSIS	NA	S	G	S
203	TESTABILITY DETAIL DESIGN AND ANALYSIS	NA	S	G	S
301	TESTABILITY DEMONSTRATION	NA	S	G	S

NOTE: PROGRAM PHASE APPLICABILITY CHANGE FROM TABLE I, APPENDIX A OF MIL-STD-2165 IS SHOWN WITH ■

CODE DEFINITIONS

CONCEPT - CONCEPT EXPLORATION

D&V - DEMONSTRATION & VALIDATION

FSD - FULL SCALE DEVELOPMENT

PROD - PRODUCTION & DEPLOYMENT

S - SELECTIVELY APPLICABLE TO HIGH RISK ITEMS DURING D&V, OR TO DESIGN CHANGES DURING PROD.

G - GENERALLY APPLICABLE

NA - NOT APPLICABLE

(1) MIL-STD-1388 IS PRIMARY IMPLEMENTATION DOCUMENT FOR DIAGNOSTIC REQUIREMENTS TRADEOFFS AND REVIEW AS PART OF LOGISTICS SUPPORT ANALYSIS DURING CONCEPT EXPLORATION PHASE.

R87-3537-004(T)

against the propagation of errors through the system. Periodic testing may be used for monitoring those functions which provide backup/ standby capabilities or are not mission critical. On-demand testing is typically used for monitoring those functions which require operator interaction, sensor stimulation, etc., or which are not easy, safe, or cost-effective to initiate automatically. The maximum permitted latency for failure detection determines the frequency at which diagnostic procedures should be run and should take into account function criticality, failure rate, possible wear out factors, and the selected maintenance concept.

Current C³I systems are capable of achieving high levels of fault detection coverage by utilizing BIT and manual aided operational tests. However, the premise of using the same test for similar elements may lull managers into thinking that redundant elements will not add to the complexity of the equipment's BIT, ATE, or manual fault detection/isolation techniques. Unless potential problem areas are cited well in advance and excellent fault tolerant techniques are included, it might become impossible to meet stringent fault detection coverage demands. Examples of such problem areas are given in para. 4.2.1 of this document. Testability tasks that require additional emphasis and tailoring in both the SOW and associated CDRLs for fault tolerant system developments are discussed in the paragraphs that follow. In addition, a number of other testability tasks which are implemented in the same way for both fault tolerant and non-fault tolerant systems have been included due to their importance in the formulation of the overall testability program.

- *Task 101, Testability Program Planning* - Although the procedures for developing and implementing a testability program are the same for both non-fault tolerant and fault tolerant systems, the success of the latter is heavily dependent upon inherent testability features (see para. 4.2.1). Therefore, the imposition of this task is recommended during the Concept Exploration phase since it provides management visibility for monitoring, control and coordination of testability design considerations between interrelated design and support activities. Submitted at the beginning of the Demonstration/Validation phase, the testability program plan should highlight the methodology to be used in establishing qualitative and quantitative testability requirements for the system specification. The plan should also describe the methodology to be used in allocating quantitative system testability requirements down to the subsystem or configuration item level. In order to establish and maintain an effective testability program, the maintainability manager must form a close liaison with all design disciplines, and must be prepared to work aggressively with design engineers to ensure a proper bal-

ance between performance, cost and supportability. It should be noted that the testability program plan may be submitted with the reliability and maintainability program plans.

- *Task 103, Testability Data Collection and Analysis Planning -*

Although much of the actual collection, subsequent analysis of data, and resulting corrective actions may occur beyond the end of the program phase under which the testability design effort is performed, it is essential that the planning for this task be initiated in the Full-Scale Development phase, preferably before the critical design review (CDR). A plan should be developed for the analysis of production test results and maintenance actions for fielded systems to determine if BIT hardware and software, ATE hardware and software, and maintenance documentation meet the specifications in terms of fault detection, fault resolution, false indications, fault detection times, and fault isolation times. Also, all data collection requirements should be defined to meet the needs of the testability analysis. The data collected should include a description of relevant operational anomalies and maintenance actions. Data collection should be integrated with similar data collection procedures, such as those for reliability and maintainability, and Logistic Support Analysis and should be compatible with specified data systems in use by the military user organization. This task is implemented in the same way for both fault tolerant and non-fault tolerant systems.

- *Task 201, Testability Requirements -* Accomplishment of this task is recommended during the Concept Exploration and the Demonstration/Validation phases. The testability requirements for this task are to establish and identify the risks and uncertainties involved in determining the performance monitoring, BIT, level of fault tolerance, repair verification, fault detection/isolation, test points, and off-line test objectives for both fault tolerant and

non-fault tolerant systems. Establishing performance requirements at the system and subsystem level should include specific numeric performance requirements imposed by the procuring activity such as:

- Maximum allowable time between the occurrence of a failure condition and the detection of the failure for each mission function
- Maximum allowable occurrence of system downtime (usually specified in percent) due to erroneous failure indications (false alarms)
- Maximum allowable system downtime due to corrective maintenance actions at the organizational level.

Testability requirements should also include the evaluation and identification of alternative diagnostic concepts which include varying degrees of BIT, manual and off-line automatic testing and diagnostic test points. These will determine the sensitivity of system readiness parameters to variations in key testability parameters which include BIT fault detection, fault isolation and false alarm rates.

- *Task 202, Testability Preliminary Design and Analysis* - It is recommended that this task be performed during the Demonstration/Validation phase, modified during the Full-Scale Development phase, and utilized to determine quantitative testability requirements that are achievable, affordable, and adequately support system operation and maintenance. The testability design techniques in this task focus primarily on the compatibility between the item and its off-line test equipment, the BIT (hardware and software) provided in the item to detect and isolate faults, and the structure of the item in terms of partitioning for enhanced fault isolation and detection. Testability design techniques, must be closely coordinated with the fault tolerant designs, and

should provide for the independent testing of redundant circuitry. Fault assessment, reconfiguration into degraded modes, and configuration verification should make maximum use of equipment redundancy and functional redundancy to assist in testing. The testability design techniques in this task will be further refined and implemented in task 203.

- *Task 203, Testability Detail Design and Analysis* - Detailed testability design is an important aspect of the design process for fault tolerant systems since inherent testability features will ultimately control hardware redundancies. This task should be accomplished in the Demonstration/Validation and Full-Scale Development phases to incorporate testability design features (including BIT) into a system or equipment design which will satisfy both testability and overall system fault tolerance requirements. This analysis should identify the failures of each component and the failures between components which correspond to the specified failure modes of each equipment to be tested. These failures represent the predicted failure population and are the basis for test derivation (BIT and off-line test) and test effectiveness evaluation. A FMEA from task 204 of MIL-STD-470 should be fully utilized as required. The FMEA requirements may need to be modified or supplemented to provide the level of detail needed. Analysis should be performed to identify the inherent levels of BIT fault detection and isolation in the design of the overall system. The false alarm rate for the overall system should also be determined by analysis. These capabilities should be compared to the requirements to see if they are suitable and adequate for the proposed design. System-level BIT hardware concepts and software architectures should be developed prior to, or while integrating, the BIT capabilities of each subsystem/item. The procedures for conducting this task on fault tolerant systems are the same as those used for non-fault tolerant systems.

- *Task 301, Testability Demonstration* - The test methods and requirements for the testability demonstration tests should be established in accordance with MIL-STD-471A (Notice 2). Through the development of the testability demonstration plan, the items to be demonstrated under the maintainability demonstration and the Test Program Set (TPS) demonstration may be coordinated (e.g., some common faults inserted) so as to provide data on the correlation of BIT and off-line test results. This can give an early indication of possible "cannot duplicate" (CND) problems in the field. The false alarm rate (an important testability parameter) is difficult to measure in the controlled environment of a demonstration procedure. If the false alarm rate was relatively high, it would be possible to make use of a reliability demonstration procedure from MIL-STD-781 to demonstrate the false alarm rate, treating each false alarm as a relevant failure. In most cases, however, the rate will be low and almost impossible to verify. Analytical techniques must then be employed. The environmental conditions during the demonstration should (if possible) be indicative of the expected operational environment in order to expose the equipment to realistic stresses.

Typical methods available to insert faults into the equipment include disconnecting leads to simulate opens, grounding pins to simulate shorts, inserting known faulty parts, removing circuit cards or wires, and by replacing a good part, circuit, or assembly with an identical item known to possess a particular type failure. The appropriate mix of these or other fault insertion techniques to be used in a testability demonstration depends upon the specific design.

Even with a reasonably large sample of inserted faults, a demonstration can yield only limited data on actual test effectiveness. However, a demonstration is also useful in validating some of the

assumptions and models used during the earlier testability analysis and prediction efforts (task 203) which may have been based upon a much larger fault set. If certain assumptions or models are invalidated by the demonstration, appropriate portions of task 203 should be repeated and new predictions should be made.

For fault tolerant systems, it is recommended that the scope of the testability demonstration be expanded or integrated with a fault tolerance verification test. The purpose of the test is to evaluate and demonstrate how well the system fault tolerant design meets requirements with respect to fault protection coverage, fault recovery time, fault types to be tolerated, maximum allowable missing data, maximum allowable corruption of data and false alarm constraints. The CDRL for the testability/fault tolerance demonstration plan should require identification of the analysis, simulation and testing procedures required to develop objective evaluation and acceptance criteria for the systems testability and fault tolerant design features.

For fault tolerant systems, the above Testability tasks should be coordinated with associated Reliability, Maintainability, Logistic Support, and System Safety tasks and analyses.

2.1.4 Software Program Tailoring

Software is a major system development driving element. Because of the importance of software in successfully attaining system performance, fault detection, fault isolation and reconfiguration, the systems manager must plan, organize, and control the software project. Although software program tailoring is implemented the same way for a fault tolerant system as for any other system, this section has been included due to the importance of software in the system life cycle. DoD-STD-2167 contains requirements for the development of mission-critical

computer system software. It establishes a uniform software development process which is applicable throughout the system life cycle. It incorporates practices which have been demonstrated to be cost-effective from a life cycle perspective, based on information gathered by the DoD and industry. Essential software development process activities that must be considered include the following:

- Project organization and planning with special emphasis on the Software Development Plan
- Resource estimation and allocation including cost, schedule, and staff
- Required document preparation and delivery
- Project monitoring and control
- Independent review and assessment of design
- Test and certification.

2.1.4.1 Management Organization and Planning Considerations - The key to successful software management is a clear understanding of the scope of the project and early emphasis directed at clarifying the requirements, the deliverables, and the organizational framework. Proper attention to these areas will ensure the system manager controls the salient elements that affect project planning. Critical questions the manager must address include:

- What functions must the system perform?
- With what other systems will this system interact?
- What documents, programs and files are specified as deliverable products?
- What criteria will be used to judge the acceptability of the final product?
- What is the procedure for incorporating requirements changes that affect the scope of the work?
- Who are key contact people from the customer, developer, and support groups?
- Do different groups understand their areas of project responsibility?

- Where will the development work be done?
- Which development computers will be used?

2.1.4.2 The Software Development/Management Plan - The software development/management plan provides a disciplined approach to organizing and managing the software project. A successful plan provides a structured checklist of important questions, consistent documentation for project organization, a baseline reference with which to compare actual project performance and experiences, and a detailed explanation of the management approach to be used.

By completing the plan early in the program, the manager becomes familiar with the essential steps for organizing the development effort, e.g., estimating resources, establishing schedules, assembling a staff, and setting milestones.

2.1.4.3 Resource Estimation and Allocation - Two of the most critical resources are development staff and time. The software manager is concerned with how much time will be required to complete the project and what staffing level will be necessary over the development cycle.

Table 2-4 is provided to give insight into a typical distribution of schedule and personnel effort in generic terms.

TABLE 2-4. Typical Distribution of Software Development Schedule & Personnel Effort By Phase.

PHASE	PERCENT OF TIME SCHEDULE	PERCENT OF EFFORT
Requirements Analysis	5	6
Preliminary Design	10	8
Detailed Design	15	16
Implementation	40	45
System Testing	20	20
Acceptance Testing	10	5
	100	100
R87-3537-005(T)		

2.1.4.4 Required Document Preparation and Delivery - Documents and deliverables provide an ongoing system description and serve as key indicators of progress. They are a major concern of software managers because they mark the transitions between life-cycle phases. Table 2-5 contains a list of DoD-STD-2167 documents and deliverables that are of specific interest to the software manager. With the exception of the Software Requirements document, all documents/deliverable identified as requiring management emphasis are also listed in DoD-STD-2167 as being the primary responsibility of management. The Software Requirements Specification warrants management emphasis since more than half of all software errors that occur are traceable back to a misstatement of software requirements.

TABLE 2-5. DoD-STD-2167 Software Documentation Requirements Matrix.

DOCUMENT	TASK PRIMARY RESPONSIBILITY	SOFTWARE MANAGEMENT EMPHASIS
System/Segment Specification*	ENG(R)	
Software Development Plan*	MGT	✓
Software Configuration Management Plan	MGT	✓
Software Quality Evaluation Plan	MGT	✓
Software Requirements Specification*	ENG(R)	✓
Interface Requirements Specification	ENG(R)	
Software Standards and Procedures Manual	MGT	✓
Software Top Level Design Document*	ENG(D)	
Software Detailed Design Document*	ENG(D)	
Interface Design Document	ENG(D)	
Database Design Document	ENG(D)	
Software Product Specification*	ENG(D)	
Version Description Document*	ENG(D)	
Software Test Plan*	MGT	✓
Software Test Description*	ENG(T)	
Software Test Procedure*	ENG(T)	
Software Test Report*	ENG(T)	
Computer System Operator's Manual	SUP	
Software User's Manual	SUP	
Computer System Diagnostic Manual	SUP	
Software Programmer's Manual	SUP	
Firmware Support Manual	SUP	
Operational Concept Document*	ENG	
Computer Resources Integrated Support Document*	MGT	
Configuration Management Plan	MGT	✓
Engineering Change Proposal*	CDM	
Specification Change Notice*	CDM	
LEGEND: ENG(R) Engineering Requirements MGT Management ENG(D) Engineering Design CDM Configuration Data Management ENG(T) Engineering Test SUP Suppliers of the Computer System R87-8011-001 * Document Usually Required R87-3537-006(T)		

2.1.4.5 Project Monitoring and Controlling Tools - A tool in the software environment is any instrument that supports the software production effort. For example, the software development/management plan, the cost estimation procedure, and the project notebook can be classified as management tools. As a minimum these tools can be utilized for software configuration management, project cost control and a project histories data base.

2.1.4.6 Independent Review and Assessment of Design - In the current era of software intensive weapon systems, success of the system requires proper operation of both hardware and software. Discovering errors early in the software life cycle yields a substantial cost savings. Software errors uncovered during the design phase are 5 to 10 times less costly to correct than errors discovered during unit and integration testing. The processes utilized to design and build high reliability software are analogous in many ways to hardware techniques. Areas of commonality include using skilled senior personnel in high risk, critical areas, in-depth design reviews by independent personnel, and extensive testing. It should be noted that Software Quality Assurance activities provide an auditing function (similar to Hardware Quality Assurance) and is not a substitute for an independent design review.

2.1.4.7 Testing and Certification - Both testing and certification are methods used to ensure quality in the delivered software. Testing identifies defects so the software can be revised before it is released. Certification subjects the product and process to independent inspection and evaluation. Certification is a statement that some requirement has been met by the product or process.

2.1.4.8 Software Development Guidelines for Testability - The software which makes a design fault tolerant (error processing routines, confidence tests, error detection/correction techniques, etc.) may be contained in the operational and/or BIT software. Guidelines for the preliminary design and analysis of software BIT can be found in the Testa-

bility Program Application Guidance of MIL-STD-2165, Appendix A, para. 50.6.7. In addition, memory sizing approximations for error-correcting techniques or reconfiguration strategies, should include memory requirements for subroutines dealing with equipment and personnel safety (operator alert and instruction) in the event of certain failure modes. A list of these failure modes may be acquired from the FMEA effort and are very helpful in pointing out critically important areas of BIT diagnostic routines.

2.2 PROGRAM PLANNING AND MANAGEMENT CHECKLIST QUESTIONS

Unless specifically noted, the checklist questions apply both to AF and contractor program managers. These questions are particularly applicable at the SRR, PDR and CDR to supplement the R&M evaluation criteria listed in MIL-STD-1521, *Technical Reviews and Audits for Systems, Equipment and Computer Software*. Questions primarily addressed to the Procuring Activity are followed by a (PA). Those addressed to integrating or prime contractors are followed by a (C).

- a. Has applicable R/M/T program tailoring and application guidance (see para. 2.1.1, 2.1.2 and 2.1.3) been incorporated in the SOW requirements for a fault tolerant system development program? (PA)
- b. Have the levels of analysis and schedule for reliability, maintainability, testability, safety and logistics tasks been consistently specified, coordinated and integrated?
- c. Does the requirement to develop mission reliability models for highly fault tolerant systems include a listing of existing computerized models that are suitable to this analysis? (PA)
- d. Has a requirement for the identification of the level at which faults can and cannot be tolerated been specified?
- e. Has software project planning been accomplished?
- f. Are the bidder's software development plans realistic in terms of the size of development staff and schedule? (PA)

- g. Are project history data bases available to assist managers in assessing performance and recognizing problems?**
- h. Has consideration been given to independent review and assessment of high risk critical design areas?**
- i. Do the bidder's plans reflect adequate resources allocated to software testing? (PA)**

**NOTE: Primary Responsibility Codes - (PA) = Procuring Activity
(C) = Prime Contractor
All others = Both**

2.3 SPECIFICATION OF FAULT TOLERANCE AND R/M/T REQUIREMENTS

Program managers must ensure that specification requirements for fault tolerance are developed as soon as practicable, preferably during the Concept Exploration phase. The requirements should be further developed and refined during the Demonstration/Validation and FSED phases to ensure that production hardware will contain the R/M/T attributes necessary for the C³I application. Quantitative requirements should be used in conjunction with specific R/M/T design requirements to provide the necessary control in the system design process. Before establishing R/M/T design specification requirements for fault tolerance, the following factors must be considered:

- System availability
- Functional criticality
- Acceptable degraded modes of operation
- Inherent reliability of lowest level of functionally redundant elements
- Diagnostic capability commensurate with reconfiguration control
- Testability of the function
- Maintenance concept employed
- System level quantitative R/M/T requirements.

Specific examples highlighting the interrelationship of these R/M/T factors with fault tolerance are contained in Section 3.

2.3.1 System Quantitative R/M/T Requirements

There are two approaches to establishing qualitative and quantitative fault tolerance requirements. The first approach (the classical top-down) involves first establishing mission requirements and then deriving fault tolerance requirements as a function of the mission, restoration, and testability design characteristics. This approach is appropriate for AF program managers who define requirements. The second approach defines the lowest level of functional element (bottom-up approach) and then establishes fault tolerance requirements in relationship to the criticality of each system function. These subsystem and lower level requirements must satisfy overall allocations of system level fault tolerance requirements. This latter approach is employed by contractors when the selected design of a fault tolerant C³I system involves extensive use of off-the-shelf equipment.

A major concern of both approaches is to achieve high system readiness (i.e., availability). Quantitative top-level fault tolerance requirements should be derived from parametric sensitivity analyses and trade-offs to optimize system readiness. The process of establishing and later refining these top-level fault tolerance requirements during the design process is outlined in para. 5.1.

The subsections that follow contain specific recommendations useful in developing R/M/T specification requirements for fault tolerant systems. In addition, AF program managers should consider the following general guidelines when deriving R/M/T system specification requirements:

- Is the requirement overspecified? (Leading to higher development, test and production costs)
- Is the wording of the requirements subject to misinterpretation?
- Is the requirement necessary, or is it included merely because of previous usage?

- Can compliance with the requirement be verified?
- Have adequate design margins (tolerance) been allowed?
- Has tailoring been considered for all referenced standards?

The exact method of specifying R/M/T depends on the equipment/system that is being developed and its ultimate application. The customary language used in system specifications must be supplemented when specifying the R/M/T of fault tolerant C³I systems. Guidance in specifying R/M/T requirements for these fault tolerant systems is provided in the following sections.

2.3.1.1 Reliability/Fault Protection Coverage Requirements - Fault tolerant systems will continue to function in the presence of faults or errors within the system. These faults and errors may result in no loss, partial loss, or complete loss of system functions. Partial loss of system functions can result in varying levels of degraded system performance.

During the Concept Exploration and Demonstration/Validation phases, program managers must consider the permissible level of system performance degradation that can be tolerated without compromising mission success. Based upon these findings, satisfactory system performance can be defined. This definition of satisfactory system performance is then included in and keyed to the Reliability Requirements Section of the C³I System Specification. If the actual C³I system operating modes are known during the Concept Exploration and Demonstration/Validation phases, they should be substituted, as applicable, in lieu of system performance levels when defining satisfactory system operation.

The following should be considered by AF program managers in preparing reliability requirement inputs to fault tolerant C³I system specifications:

- a. Quantitative mission reliability
- b. Quantitative maintenance frequency reliability
- c. Description of storage, transportation, operation and maintenance environments

- d. Time measure or mission profile
- e. Definition of satisfactory and acceptable degraded system performance
- f. Tolerable failure policy (Single-point failure, fail-safe, etc.)
- g. Failure independence
- h. Critical mission definition.

Items a thru e above are the normally specified reliability inputs to system, prime-item development and lower-tier development specifications. Paragraphs 6.2 and 12.3.1 of MIL-HDBK-338 provide guidance and examples for preparing these reliability specification inputs. Items f thru h are additional recommended specification inputs for fault tolerant systems.

Item b, the quantitative maintenance frequency reliability, is specified in operational/field terms (e.g., Mean-Time-Between-Maintenance-Action (MTBMA) and Mean-Time-Between-Maintenance-Inherent (MTBMI) in major system specifications in accordance with Department of Defense Directive 5000.40, *Reliability and Maintainability*. Maintenance frequency reliability may be specified in terms of operational/field and/or contractual terms (e.g., Mean-Time-Between-Failure (MTBF)) in lower-tier development and equipment specifications. Operational/field requirements relate to maintenance organization needs for field equipment and are based on the performance of existing systems and a validated degree of design and technology improvement that can be provided at a reasonable cost. Contractual requirements are based on the inherent design characteristics and are related to the mission needs of the operating organization. The terms MTBF and mean-time-to-repair (MTTR) are exclusively contract terms and are often verified by R&M demonstration tests.

The difference between operational/field and contractual requirements is described in DoD Directive 5000.40, *Reliability and Maintainability*, and in Reference 2, and is best illustrated by comparing the parameters MTBMA and MTBF. MTBF is calculated using equipment operating

time and chargeable failures (which exclude e.g., induced failures, no-defect actions, and minor corrosion maintenance actions). The MTBMA of the same equipment might be calculated using a different time base (e.g., flight time) and would include maintenance events such as induced failures, no defect actions and minor corrective maintenance actions. The specification of operational/field R&M requirements as being separate and distinct from contractual requirements is not unique to fault tolerant systems. However, program managers of fault tolerant systems are advised to pay particular attention to this distinction in view of the emphasis placed on meeting numerical R&M requirements. In general, AF program managers should insure the following when specifying maintenance frequency reliability:

- Operational/field terms to be distinguished from contractual terms
- Numerical traceability from operational/field terms to contractual terms
- Consistency established and maintained between operational/field and contractual requirements.

Item e, the definition of satisfactory and acceptable degraded system performance, applies to quantitative mission reliability which may be expressed in terms of mission-time-between-critical-failure (MTBCF) or probability of mission success (R_M). In some cases the definition of system failure may be preferable to specifying the definition of satisfactory performance. Or, depending on the situation, including both definitions may be useful. Program managers should emphasize two objectives in developing a definition of satisfactory and acceptable degraded system performance. The first objective is to remove any ambiguity from the interpretation of quantitative reliability requirements and their method of verification. Secondly, by properly defining an acceptable level of degraded performance, a design containing unnecessary system complexity may be avoided.

A clear, unequivocal definition of "failure" must be established for the equipment or system relative to its important performance parameters. Successful system (or equipment) performance must be defined and expressed in terms which will be measurable during the demonstration test. Parameter measurements during the demonstration tests usually include both go/no-go performance attributes and variable performance characteristics. Since fault tolerant systems are often designed to degrade gracefully (see para. 4.1.7), the limits of acceptable performance, which are usually set at levels below which a mission may be degraded beyond an acceptable level, should be established prior to testing. Failure of go/no-go performance attributes such as channel switching, target acquisition, target classification, etc., are relatively easy to define and measure to provide a yes/no decision boundary. Failure of a variable performance characteristic, on the other hand, is more difficult to define in relation to the specific limits beyond which system performance is considered unsatisfactory.

Figure 2-2 illustrates the two types of performance characteristics and corresponding success/failure (yes/no) decision boundaries that might be applied to a track radar or to a missile active seeker (guidance) system. In both cases, the success/failure boundary must be determined for each essential system performance characteristic measured in the demonstration test. They must be defined in clear, unequivocal terms. This will minimize the chance for subjective interpretation of failure definition, and post-test rationalization (other than legitimate diagnosis) of observed failures.

The criticality of the C³I system or certain of its functions often dictates that design requirements be set forth for tolerable failure policy and failure independence. Therefore, consideration should be given to specifying fail-safe/fail-operational design and prohibiting single-point failures.

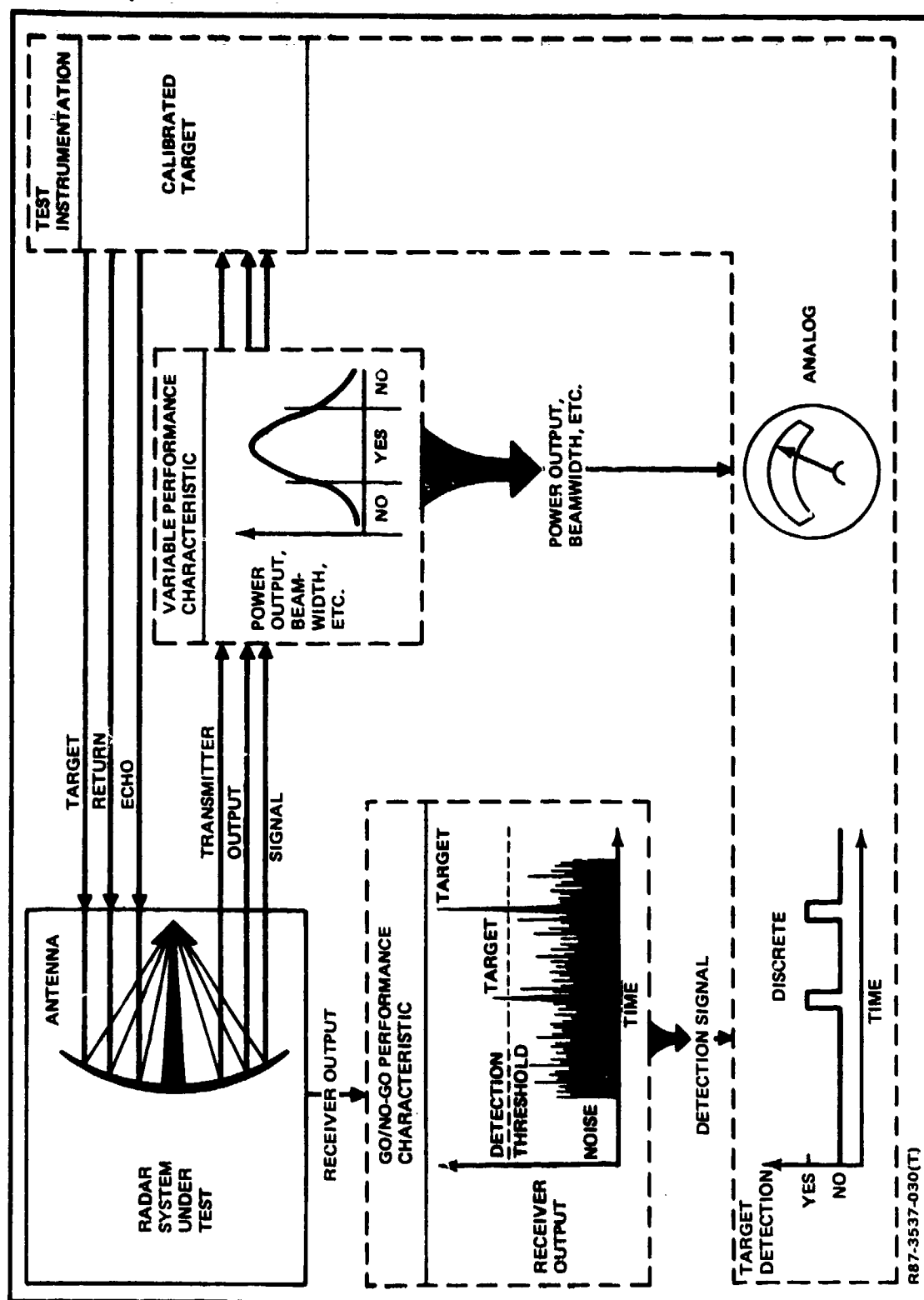


Figure 2-2. Verification of System Performance Characteristics.

Failure independence requirements may stipulate fault containment or fault propagation restrictions to limit both the immediate effects of faults and possible secondary failure effects. When specifying a tolerable failure policy or failure independence requirements, be sure to include the equipment level to which the requirement applies. For example, if redundant subsystems were used, faults would be tolerated at the subsystem level. The system level is above that at which the faults would be tolerated while the assembly or card level would be below that at which faults would be tolerated.

C³I systems may contain many operating modes and functions some of which are used in peacetime and some in wartime. In such cases, it is recommended that a critical mission capability (that is tied to an essential mission performance level) be defined. This definition could then be related to quantitative reliability and availability requirements and their respective demonstrations/verifications.

Figure 2-3 provides two examples of the reliability specification of fault tolerant C³I systems. The first example is of a C³I data fusion system made up of existing off-the-shelf computers and other equipment. The second is a fault tolerant flight control computer used on a C³I platform.

2.3.1.2 Fault Protection Coverage - Fault protection coverage is a concept that can be stated in both quantitative and qualitative terms. The quantitative statement is used most often in reliability modeling of reconfigurable or redundant systems. The output of these reliability models, the probability of system success, has been found to be quite sensitive to the fault protection coverage parameter. In its quantitative sense, fault protection coverage is the conditional probability that the system successfully recovers when a specific type of failure has occurred. What constitutes proper recovery is a direct function of the in-

EXAMPLE 1: C³I DATA FUSION SYSTEM

RELIABILITY

FAIL SAFE DESIGN — The XYZ system shall not have any single point failures in the critical path (i.e., the design shall compensate for a failure by redundancy or an alternate operating procedure to insure the continued flow of message traffic). A critical path is defined as any path within the XYZ system which is necessary for the continued data flow.

This is an example of a tolerable failure policy applicable to the system level. Also included is a reference to a critical path which defines the system's essential functional requirements.

MISSION RELIABILITY — The mission time-between-critical-failure (MTBCF) shall be no less than xxx hours when operated under the environmental conditions specified herein. The design of the XYZ system shall result in a predicted MTBCF equal to or exceeding twice (as a rule-of-thumb) the specified MTBCF. A critical failure is defined as any failure in which a critical mission capability is not restored in less than yyy milliseconds.

This is an example of specifying MTBCF rather than probability of mission success (R_{MS}). In addition, the mission criticality is such that a maximum time is specified to restore (via redundancy or alternate operating procedure) the critical mission capability.

MAINTENANCE FREQUENCY RELIABILITY — The mean time between (corrective) maintenance (MTBM) actions, as defined in AFR 80-18 of the XYZ system, shall be no less than zzz hours. The design of the XYZ system shall result in a predicted MTBM equal to or exceeding twice the specified MTBM.

This is an example of specifying an operational or field reliability parameter as measured by the AF 66-1 Maintenance Management System. Verification or demonstration of this requirement normally would be accomplished using field data during initial deployment. Another approach could be to specify a minimum acceptable system MTBF verified by a MIL-STD-781 demonstration test.

INDEPENDENCE OF FAILURE — The XYZ system shall be designed such that a unit level failure can not induce any other failure.

CRITICAL MISSION CAPABILITY — Critical mission capability is that level of performance which shall allow the XYZ system to perform its mission of supporting the required communications and information flow without degradation. The following XYZ functions shall be operating in order for the system to meet critical mission capability...

This is an example of a complex system wherein it is necessary to tie the quantitative mission reliability requirement to an essential mission performance level.

EXAMPLE 2: FAULT TOLERANT AIRBORNE AVIONICS SYSTEM

RELIABILITY — The XYZ system shall have a predicted reliability (as specified below) based on analysis in accordance with MIL-HDBK-217. This includes all components of redundant circuits employed to achieve fault tolerance. The predicted reliability under the temperature and altitude conditions specified herein for continuous operation, shall be not less than:

- a. Mean Time Between Failures (MTBF) = xxx hours (includes failures in redundant circuits)
- b. Mission Time Between Critical Failures (MTBCF) = yyy hours (System Fail-Operational capability maintained) (see Level of Fault Tolerance below)

NOTE: When a malfunction is detected, it is assumed that maintenance to restore full fault tolerance capability occurs after each mission or the first available time.

MAINTENANCE FREQUENCY RELIABILITY — The mean time between corrective maintenance action of the XYZ system shall be no less than zzz flight hours.

R87-3537-029(1/2)(T)

Figure 2-3. Examples of Reliability Specification of Fault Tolerant Systems. (Sheet 1 of 2)

INDEPENDENCE OF FAILURE — The XYZ system shall be designed such that at the ABC (e.g., subsystem, unit, assembly, LRU, SRU) level no failure shall induce any other failure.

FAULT TOLERANCE REQUIREMENTS — The XYZ system shall provide a fault tolerant performance capability in compliance with the contractual statement of work, and in accordance with the following criteria.

LEVEL OF FAULT TOLERANCE — This capability shall specify the system (or subsystem, by function) response to any randomly occurring single fault, or sequence of unrelated faults. Failure is defined as any situation, detected by any means, in which the XYZ system does not meet specification requirements during operation. The applicable levels for a single fault are:

- a. **Fail-Safe:** XYZ system output data frozen or disabled — failure annunciated — before any variable error exceeds 2x specified accuracy.
- b. **Fail-Operational:** XYZ system output data continues uninterrupted — status change annunciated — transient disturbances do not exceed 2x specified accuracies.

The response of the Fail-Operational system to each subsequent fault in a sequence shall result in no less than the following system state (provided by redundancy or a degraded operating mode):

Fail-Operational/Fail-Safe — (System state complies with Fail-Safe criteria)

FAULT PROTECTION COVERAGE — At the "FAIL-SAFE" level, the effectiveness of the XYZ system shall not be less than (VV) percent for a two-hour sortie.

EFFECTIVENESS OF FAULT TOLERANCE — A Failure Mode and Effects Analysis (FMEA) shall be performed to determine the effectiveness of the fault tolerant design. Component and functional area failure probabilities shall be calculated for the XYZ system's MTBF and MTBCF.

R87-3537-029(2/2)(T)

Figure 2-3. Examples of Reliability Specification of Fault Tolerant Systems. (Sheet 2 of 2)

tended criticality of the application. It may mean merely establishing a workable hardware system configuration (such as communications switching processors), it may require that data flow not be interrupted (such as a satellite attitude control system computer), or it may mean error free processing (no erroneous results are output from the processing element). The formulation of the probability of recovery, i.e., establishing a workable system configuration, can be illustrated if one considers the case of a communications system containing a number of active and standby spare processors. If one active processor fails, the probability of recovery would be equal to the joint probability of correct fault detection and correct fault isolation, and the switching over to a backup spare processor and that the backup spare successfully restores operation (e.g., boots, loads from memory and resumes process).

A second, more limited quantitative definition of fault protection coverage relates to the probability of detecting any fault. The value of fault protection coverage can be determined by using the average of the coverages for all possible classes of failures weighted by the probability of occurrence of each fault class.

A third, more limited, quantitative definition of fault protection coverage is the probability that a particular class of fault is successfully detected before a complete system failure occurs. *Fault classes* include the following: latent, permanent, transient, intermittent, catastrophic, common cause, design, and single point.

The qualitative meaning of fault protection coverage specifies the types of errors against which a particular redundancy scheme guards. For example, the coverage of Hamming single-error-correcting, double-error-detecting code is the correction of all single-bit errors in a code word, and the detection of all double bit errors and some multiple bit errors.

The specification of fault protection coverage can take many forms starting with the top level system specification and working down to lower level specifications. The top level system specifications usually specify fault protection coverage as follows:

"FAULT PROTECTION COVERAGE - All fault classes for the XYZ system shall be covered except for the following (e.g.):

- 1. Generic faults which affect all processor channels in an identical manner***
- 2. Multiple faults, i.e., faults which affect multiple processor channels simultaneously***
- 3. Faults which occur during reconfiguration."***

In addition to, or in lieu of, the qualitative form of specifying fault protection coverage, lower level prime item development/equipment specifications may include a quantitative requirement for fault protection coverage by taking the form:

"FAULT PROTECTION COVERAGE - The fault protection coverage (FPC) of the XYZ subsystem shall not be less than xxx percent. Fault protection coverage is the combination of the independent probabilities of Fault Detection (FD), Fault Isolation (FI), and Fault Recovery (FR) for all possible faults of the system."

2.3.1.3 Maintainability/Testability Requirements - An excellent guide to these requirements is provided in Appendix A, para. 40.1.1 of MIL-STD-470A, *Maintainability Program for Systems and Equipment* particularly those that pertain to identifying and quantifying maintainability needs. This data is a recommended reference guide before undertaking this task. All operational and deployment constraints, listed in para. 40.1.1.2 of MIL-STD-470A as fundamental to the user's needs, are of particular importance to a manager wrestling with redundancy versus corrective maintenance tradeoffs.

Another excellent guide is provided in Appendix A, paras. 50.5.6 and 50.5.7 of MIL-STD-2165, *Testability Program for Electronic Systems and Equipment*. These guidelines pertain to testability requirements which must be considered for inclusion in a system specification. Figure 5 of that Appendix A is shown here as Fig. 2-4 and lists 13 model requirements (a thru m) for system testability. Two additional recommended model requirements (n) and (o) are also listed in Fig. 2-4. In certain C³I system applications a manual error recovery requirement (n) may be a necessary addition to automatic error recovery (model requirement (l)). Manual error recovery should make maximum utilization of the hardware and software implemented for requirement (a), status monitoring, to alert an operator or crew member to execute an error recovery action. Typical operator actions may include manually switching to a backup operating mode, correcting the error by replacing an easy access, plug-in module, or by temporarily continuing system operation in a degraded operating mode. Air Force and contractor program managers of fault tolerant system development efforts should consider the following guidance applicable to two (l and m) of these model requirements.

Automatic error recovery methods such as reconfiguration, error correction code, checkpoint rollback, redundant message sending, and/or retry may be incorporated in fault tolerant designs. It is important that wherever possible, the specified requirement for automatic error recovery (l) be coordinated with and make use of the planned hardware and

3.X.X Design for testability

- a. Requirement for status monitoring.
- b. Definition of failure modes, including interconnection failures, specified to be the basis for test design.
- c. Requirement for failure coverage (% detection) using full test resources.
- d. Requirement for failure coverage using BIT.
- e. Requirement for failure coverage using only the monitoring of operational signals by BIT.
- f. Requirement for maximum failure latency for BIT.
- g. Requirement for maximum acceptable BIT false alarm rate; definition of false alarm.
- h. Requirement for fault isolation to a replaceable item using BIT.
- i. Requirement for fault isolation times.
- j. Restrictions on BIT resources in terms of hardware size, weight and power, memory size and test time.
- k. Requirement for BIT hardware reliability.
- l. Requirement for automatic error recovery.
- m. Requirement for fault detection consistency between hardware levels and maintenance levels.
- *n. Requirement for manual error recovery.
- *o. Requirement for the identification of the level for which faults can and cannot be tolerated.

*Additional recommended requirements which are not presently included in MIL-STD-2165.

R87-6011-603
R87-3637-008(T)

Figure 2-4. Model Requirements for Testability in a System Specification.

software intended to fulfill requirements (d), (e) and (h). The specification of automatic fault recovery methods should include the following as applicable:

- Identification of the fault classes (see para. 2.3.1.2) to which the particular recovery methods apply
- Specific maximum allowable recovery time.

Requirement (m), for fault detection consistency between hardware sizing and partitioning levels vs. maintenance replacement levels, should be specified in conjunction with requirement (h), the requirement for fault isolation to a replaceable item using BIT. This recommended practice will aid the BIT designer in a clearer understanding of the replaceable unit assembly level to which he should be isolating (e.g., subsystem, LRU, SRU, component, etc.). This will avoid duplication of efforts between the BIT and ATE programs.

Table 2-6 presents a typical format covering numerical requirements (a), (c), (d), (e), (g), (h) and (i) of Fig. 2-4 as well as many other testability and maintainability parameters of interest. This Notational Diagnostic Performance Specification is recommended in Reference 3 to be a deliverable item after both the Demonstration/Validation phase and the Full-Scale Development phase. By accurately quantifying all the listed parameters of this specification, a meaningful assessment can be made of a fault tolerant C³I system's testability and maintainability.

2.3.2 Verification

All contractual R/M/T requirements must have a contractually specified method of verifying compliance. There are several measures which quantify the numerical R/M/T requirements in both contractual and operational terms. These must be distinguished from each other in documenting the requirements and the associated verification method.

Contractual specifications must delineate the analysis methods and demonstration tests that must be performed to verify that the specified

TABLE 2-6. Notational Diagnostic Performance Specification.

LEVEL OF MAINTENANCE ¹	DIAGNOSTIC CAPABILITY ¹	FAULT DETECTION COVERAGE ^{2,4}	FAULT ISOLATION COVERAGE ^{2,4}	MEAN TIME TO DIAGNOSE	FALSE ALARM RATE ³	FALSE REMOVAL RATE ³	OTHER REQUIREMENTS ¹
ORGANIZATIONAL	STATUS MONITOR	_____ %	_____ %	_____	_____	_____	_____ % OF FAULT COVERAGE BY STATUS MONITOR FOR MISSION-CRITICAL FUNCTIONS BIT MEMORY ALLOCATION NOT TO EXCEED X WORDS TECHNICAL INFORMATION ACCESS TIME
	BIT	_____ %	_____ %	_____	_____	_____	
	MANUAL TEST	_____ %	_____ %	_____	_____	_____	
	MAINT. AIDS/ MANUA TROUBLE-SHOOTING	_____ %	_____ %	_____	_____	_____	
	TOTAL:	100 %	100 %				
INTER-MEDIATE	EXTERNAL ATE/ EXPERT SYSTEM	_____ %	_____ %	_____	_____	_____	ATE LIMITED TO X LB. Y CUBIC FT.
	MANUAL TEST	_____ %	_____ %	_____	_____	_____	
	TOTAL:	100 %	100 %				
DEPOT	EXTERNAL ATE	_____ %	_____ %	_____	_____	_____	
	MANUAL TEST	_____ %	_____ %	_____	_____	_____	
	TOTAL:	100 %	100 %				
1. LISTED BY WAY OF EXAMPLE 2. UNAMBIGUOUS PERCENTAGE OF FAULT DETECTION COVERAGE (RATIO OF FAILURES DETECTED TO FAILURE POPULATION) FOR EACH CAPABILITY SHOWN. TOTAL AT EACH LEVEL OF MAINTENANCE SHOULD ADD TO 100% OF THE IDENTIFIED REPLACEABLE ITEMS FOR THAT LEVEL. 3. RELATE RATES TO OPERATIONAL USAGE (E.G., 1 FALSE ALARM PER MONITORING HOUR). 4. FOR EACH DIAGNOSTIC CAPABILITY LISTED, INDICATE WHETHER "P" - PRIMARY MODE OR "S" SECONDARY OR AUGMENTING MODE. R87-5011-002 R87-3537-009(T)							

requirement has been met. For demonstration tests, the specification should define the following:

a. How will the equipment/system be tested?

Test conditions, environmental conditions, test measures, length of test, equipment operating conditions, accept/reject criteria, test reporting requirements, etc.

b. Who will actually perform the tests?

Contractor, Government, or independent organization

c. When will the tests be performed?

Development, production, or field operation phases

d. Where will the tests be performed?

Contractor's plant, Government organization, or field.

The planned R&M growth of the system, if any, must also be considered and related to the schedule for the demonstrations. If analysis shows meaningful R&M growth between the scheduled demonstration periods and system maturity, consideration should be given to specifying these initial quantitative R&M requirements in the System Specification. It may be necessary to conduct several time-phased system level R&M demonstrations at major program milestones of a C³I system development effort. If meaningful R&M growth is expected during this period, the AF program manager should consider specifying numerical R&M requirements as part of R&M growth curves. These R&M growth curves should be incorporated in the requirements section of the System Specification.

Fault detection/isolation, reconfigurability and self-healing performance as well as the maintainability/repair philosophy should be validated as early in the development as possible in order to demonstrate fault protection coverage. Traditionally, this has been accomplished at the end of the Full-Scale Development phase, which promotes a reluctance to rectify problems because both the contractor and the procuring agency are anxious to begin production and get the product into service. Thus, problems such as excessive false alarms, too many "cannot be duplicated" and "retest ok's", etc. are not properly resolved. Program managers should attempt to avoid such problems by validating high risk areas early in the development phase where corrective actions have minor impact on cost or schedule.

Exhaustive simulation and testing should be accomplished on representative high risk hardware elements as early as possible in the development cycle. It is important to cull out design deficiencies in a planned approach so that modifications and changes in test strategies can be implemented while the design is still in its infancy. To this end, AF program managers should require the contractor to document the planned approach for evaluating and demonstrating how well a fault tolerant design meets its specified fault tolerance goals and requirements. This is accomplished by including a requirement in the C³I system SOW for such tests to be identified and described in the System Test Plan, Qualifica-

tion Test Plans, Engineering Development Test Plans, Testability Demonstration Plan, and Reliability Development/Growth Test Plans, as applicable.

Provisions should be made for a maturation plan for activities as each program phase progresses. The plan should provide for:

- Comparative analysis between test methodologies and Maintainability/Diagnostic philosophies of the proposed system and similar systems already fielded
- A means to improve the proposed system by utilizing lessons learned and deficiencies of prior generation systems
- A schedule of the demonstration/validation milestones and resources required to perform these maturation activities (e.g., prime hardware, laboratory facilities, etc.)
- Establishment of a testability and maintainability performance data collection system
- Evaluation of false alarms and false removals in the system's actual or simulated environmental profile conditions
- Evaluation of diagnostic support equipment
- Testability and maintainability maturation profiles should include periodic summaries of performance throughout the development cycle as well as the results of the verifications.

2.3.3 Warranties

The inclusion of reliability improvement warranties (RIW) in requests for proposals and production procurement contracts will be a major contributor to the success of complex fault tolerant military hardware programs. Initially, these warranties provide, prior to contract award, a realistic basis for evaluating the reliability of the equipment proposed by the seller. The procedures for implementing RIWs on fault tolerant designs are similar to those used for non-fault tolerant system procurements. However, the seller's response to, and especially the pricing of the warranty for a fault tolerant system, will be a direct measure of the seller's assessment of, and confidence in, the ability of the equipment to

meet the stringent R&M requirements imposed on fault tolerant systems. Later, the RIW will provide the procuring activity with no-cost engineering change proposals (ECPs) which will improve reliability and provide higher system availability and operational readiness.

It may seem incongruous to include RIW requirements in the procurement contracts for fault tolerant systems considering the total high reliability of such systems. But it must be realized that the components of the system have finite reliabilities and will at times fail. Therefore, it is mandatory in the deployment of fault tolerant systems that those components be repaired or replaced very rapidly.

To accomplish this, a fundamental design feature of fault tolerant systems should include extensive internal monitoring and self-testing of each major component of the system during operation. In systems that perform a critical function, these self-tests are performed prior to initiating that function. If a failure is detected, the function is not initiated and possibly the mission aborted or vital data lost. In either case the detected faults are recorded for display to the line maintenance crew. Because of the national security considerations attendant to C³I systems, every effort must be made to eliminate unreliable systems components which could reduce operational readiness and cause excessive system downtime. For these reasons, AF program managers should consider including RIW requirements in requests for proposals and production contracts for fault tolerant systems. Typical parameters warranted include MTBF and BIT false alarm rates.

Competitive bid reliability incentive and warranty programs motivate contractors to provide equipments with the highest practical reliability and operational readiness. These incentive and warranty programs focus on the contractor's essential tasks and responsibilities and the Government's major concerns viz., equipment reliability and operational readiness. Further background and details of reliability warranties are provided in the *Fault Tolerant Design Implementation Guide*.

2.4 SPECIFICATION CHECKLIST QUESTIONS

The following questions are intended to ensure that program managers incorporate appropriate fault tolerance requirements into system specification documentation.

- a. What are the overall contractual reliability, maintainability and availability requirements? How do fault tolerance requirements impact the overall reliability, maintainability, and availability requirements?
- b. Has the definition of satisfactory system performance or system failure been specified? (PA)
- c. Have the maximum off-line or reconfiguration time(s) been specified or included in the definition of satisfactory performance? (PA)
- d. Has the maximum allowable missing data been specified?
- e. Has the maximum allowable contamination or corruption of existing data been specified?
- f. Have the allowable fault propagation requirements been specified?
- g. What is the tolerable failure policy? (single-point, fail-safe, etc.) (PA)
- h. Have the fault classes to be tolerated been specified? (C)
- i. What is the level of fault protection coverage required for the system? (C)
- j. Have the false alarm constraints been specified?
- k. Will the fault tolerance policies and methodologies be among the vital functions of the program to be evaluated and verified?
- l. How will the fault protection mechanisms be demonstrated or validated?
- m. Under what environmental conditions must the system be operated and maintained? The more difficult the environment for both operating and replacing of an item, the more cost-effective redundancy becomes.
- n. How critical is it that the proposed system survive the effects of natural and weapons enhanced radiation environments? (PA)

- o. What is the maximum allowable Mean Time to Restore the system?
As this time becomes shorter, the greater the need to require redundancy, particularly on those items within the system which have larger Mean Time to Repair figures.
- p. What similar systems already developed can be studied to extract some of the specifications required and cite areas for improvement? (PA)
- q. What functions in the system involve the most risk to mission success if they were to fail? The greater the risk, the greater the demand for redundancy. (C)
- r. Has a requirement for manual error recovery been properly specified if this technique is to be used?
- s. Has the level at which faults can and cannot be tolerated been specified? (PA)
- t. Has consideration been given to including an RIW requirement in the RFP for the production phase contract? (PA)

3 - RELATIONSHIP OF C³I FAULT TOLERANCE TO MISSION AND SAFETY CRITICALITY

Fault tolerance requirements for C³I systems are established to assure the availability of critical mission functions and to avoid potential safety hazards. This section describes the methodology used to identify mission and safety critical functions of complex systems and establish their fault tolerance requirements. Presented herein are several examples of fault tolerant design approaches used in C³I systems. These examples illustrate areas where fault tolerant designs may be used and where the mission operational benefits can be derived.

3.1 FORMULATION OF C³I FAULT TOLERANCE REQUIREMENTS

The deterrence of nuclear conflict, control of forces and employment of weapons all strongly depend on C³I. Because of this dependence and its importance, C³I systems must be designed to be fault tolerant in order to become survivable and available. The level of fault tolerance depends upon the operational mission, its relationship to national security and the system availability and safety requirements. Fault tolerance must be judiciously implemented to avoid unnecessary program costs and logistic support requirements for spares and maintenance personnel.

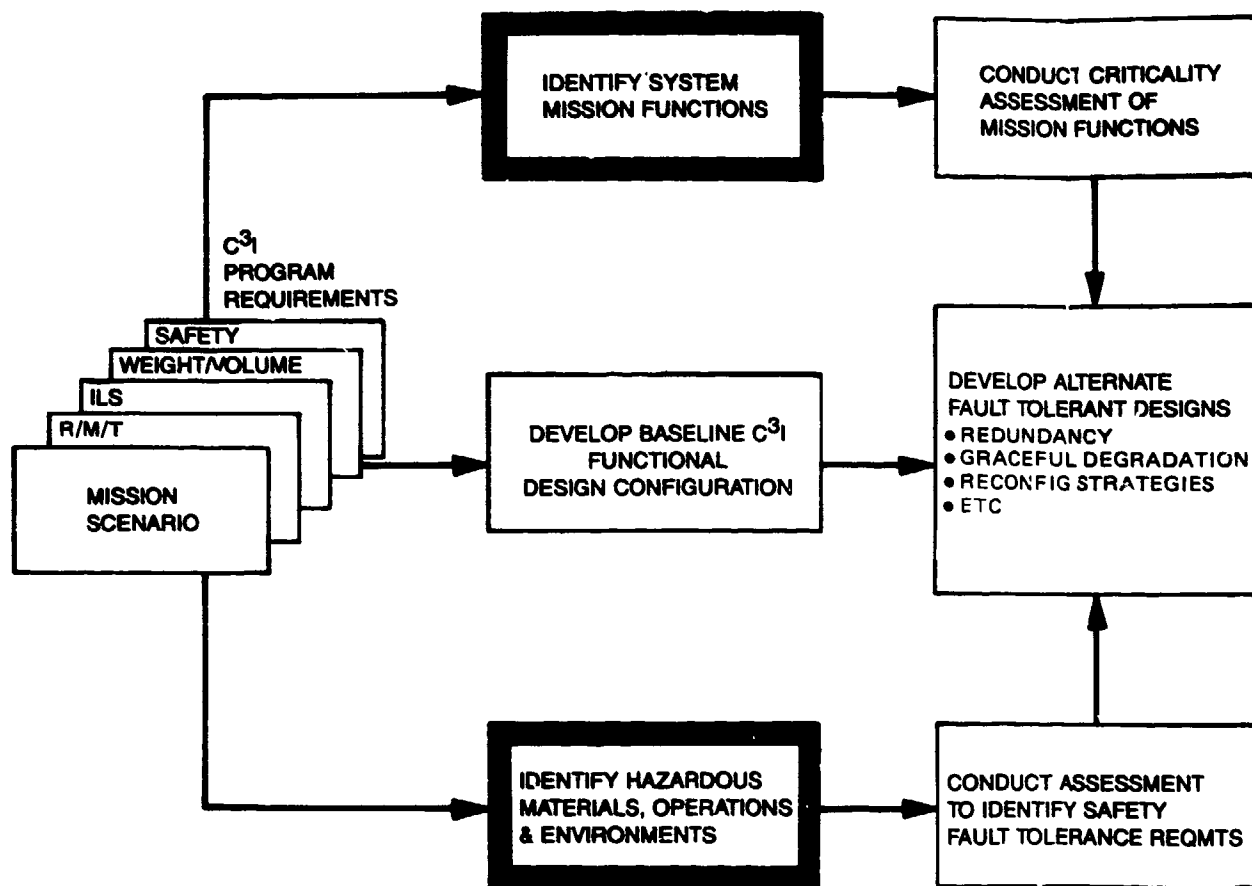
Fault tolerance requirements are normally established by the contractor in compliance with the system specification and are used by designers to develop subsystem configurations. Ultimate AF design control of this process is exercised by approval of the design concept at PDR and the design details at CDR.

Figure 3-1 illustrates how the mission and safety-critical fault tolerance requirements are established. For the mission-related requirements, the various functions of the C³I system under consideration are identified and the consequences of the loss or degradation of each function assessed. This evaluation considers the effect on the C³I systems capability and on the overall C³I community, i.e., its impact on National security, thereby permitting the establishment of functional criticality prioritization and the cost effective application of fault tolerance requirements.

It is essential that AF program managers assure themselves that the contractor's methodology and criticality assessment of mission functions are correct, since this assessment forms the basis for major program expenditures in manpower, equipment, testing, and future logistic resources.

The criticality of a C³I function is driven by its application. For example, the ability to guide weapons has the highest functional criticality of an airborne surveillance radar system. However, it is far less functionally critical to the national security when this functional capability is compared to the strategic missile detection capability of an infrared (IR) sensor system aboard a space surveillance system satellite. By establishing a hierarchy of criticality among C³I functions, each system function can be ranked in terms of its overall C³I military importance.

Applying this rationale, an IR sensor satellite designed to provide early warning detection of hostile strategic missile launches requires higher levels of fault tolerance than a satellite designed to provide meteorological information for use in guiding troop movements. The cost of restoration or repair can influence functional criticality, assuming that the function loss or system downtime can be tolerated. It may be more



CRITICALITY OF FUNCTIONS

STATE DESIGNS
RADIATION STRATEGIES

ASSESSMENT
SAFETY
REQUIREMENTS

CRITICALITY ASSESSMENT OF MISSION FUNCTIONS

C ³ I MISSION FUNCTIONS	EFFECT OF LOSS OF FUNCTION	IMPACT ON NATIONAL SECURITY	FUNCTIONAL CRITICALITY
DETECTION OF ENEMY MISSILE LAUNCH PLUMES	LOSS OF EARLY WARNING CAPABILITY FOR MISSILE ATTACK	ENEMY FIRST STRIKE POSSIBLE WITH MAJOR LOSSES	NATIONAL SECURITY

SAFETY ASSESSMENT

C ³ I EQUIPMENT	HAZARDOUS MATERIAL/ OPERATION/ENVIRONMENT	WORST POSSIBLE CONSEQUENCE	HAZARD CRITICALITY	SAFETY DESIGN REQUIREMENTS
RADAR	RF RADIATION EXPOSURE TO GROUND PERSONNEL DUE TO INADVERTANT TURN-ON OF TRANSMITTER	FATAL	CATASTROPHIC	<ul style="list-style-type: none">• DUAL REDUNDANT WEIGHT ON-WHEELS INTERLOCK• THREE POWER CABLE SWITCHES FOR TURN-ON

Figure 3-1. Identification of Mission & Safety Critical Fault Tolerance Requirements.

cost-effective to add an additional layer of redundancy to a potentially weak link in a satellite (e.g., battery, sensor, etc.) than to run the risk of the satellite's premature failure.

The safety related fault tolerance requirements are established based upon analysis of the system's potential hazards. These conditions can be determined by identifying all hazardous materials, the systems anticipated operational use and the natural and induced environmental exposure. A safety assessment can be conducted, as illustrated in Fig. 3-1, to establish the safety design requirements. This evaluation method is an extension of the efforts described in the preliminary hazard list (Task 201 of MIL-STD-882) and is performed by system safety engineers. The safety assessment is conducted very early in the system acquisition life cycle with emphasis on identification of fault tolerance provisions for hazardous areas. The analyst reviews each C³I subsystem or equipment to determine if potential safety hazards can occur as a result of hazardous material, operational use, environment, or other conditions. A hazard criticality is established based on worst-case conditions and the potential for personnel injury or damage to the system using the following definitions from MIL-STD-882:

DESCRIPTION	CATEGORY	MISHAP DEFINITION
CATASTROPHIC	I	DEATH OR SYSTEM LOSS
CRITICAL	II	SEVERE INJURY, SEVERE OCCUPATIONAL ILLNESS, OR MAJOR SYSTEM DAMAGE
MARGINAL	III	MINOR INJURY, MINOR OCCUPATIONAL ILLNESS, OR MINOR SYSTEM DAMAGE
NEGLIGIBLE R87-3537-011(T)	IV	LESS THAN MINOR INJURY, OCCUPATIONAL ILLNESS, OR SYSTEM DAMAGE

The safety engineer will then establish safety design criteria, including fault tolerance provisions that are based on the hazard severity, a qualitative assessment of the hazard probability and the C³I program system safety requirements.

Air Force and contractor program managers should carefully assess the contractor's rationale for establishing safety related fault tolerance

TABLE 3-1. Typical Functional Criticality Prioritization.

SYSTEM FUNCTION	FUNCTIONAL CRITICALITY
WEAPON GUIDANCE	1 (HIGHEST)
ATTACK CONTROL	2
SYNTHETIC APERTURE RADAR IMAGERY	3
FIXED TARGET IDENTIFICATION	3
CLUTTER MAP	3
SMALL AREA - TARGET CLASSIFICATION	3
ATTACK PLANNING	4
SECTOR SEARCH	5
WIDE AREA SURVEILLANCE	6 (LOWEST)
R87-5011-003 R87-3537-024(T)	

requirements. It may be advisable to re-evaluate the C³I program system safety requirements in light of the evaluation results so that the program objectives can be achieved without compromising system safety.

Section 4 describes the fault tolerance design options that can be implemented to satisfy the established fault tolerance requirements, and summarizes their inherent advantages and disadvantages. Tradeoffs of design alternatives are contingent on optimizing the LCC and system effectiveness as described in Section 5.

3.2 EXAMPLES OF TYPICAL C³I FAULT TOLERANCE APPLICATIONS

In this subsection, two types of fault tolerant systems are discussed; a space surveillance system and an airborne radar system. These are used to illustrate how various fault tolerance approaches can be applied to effectively enhance C³I mission capabilities.

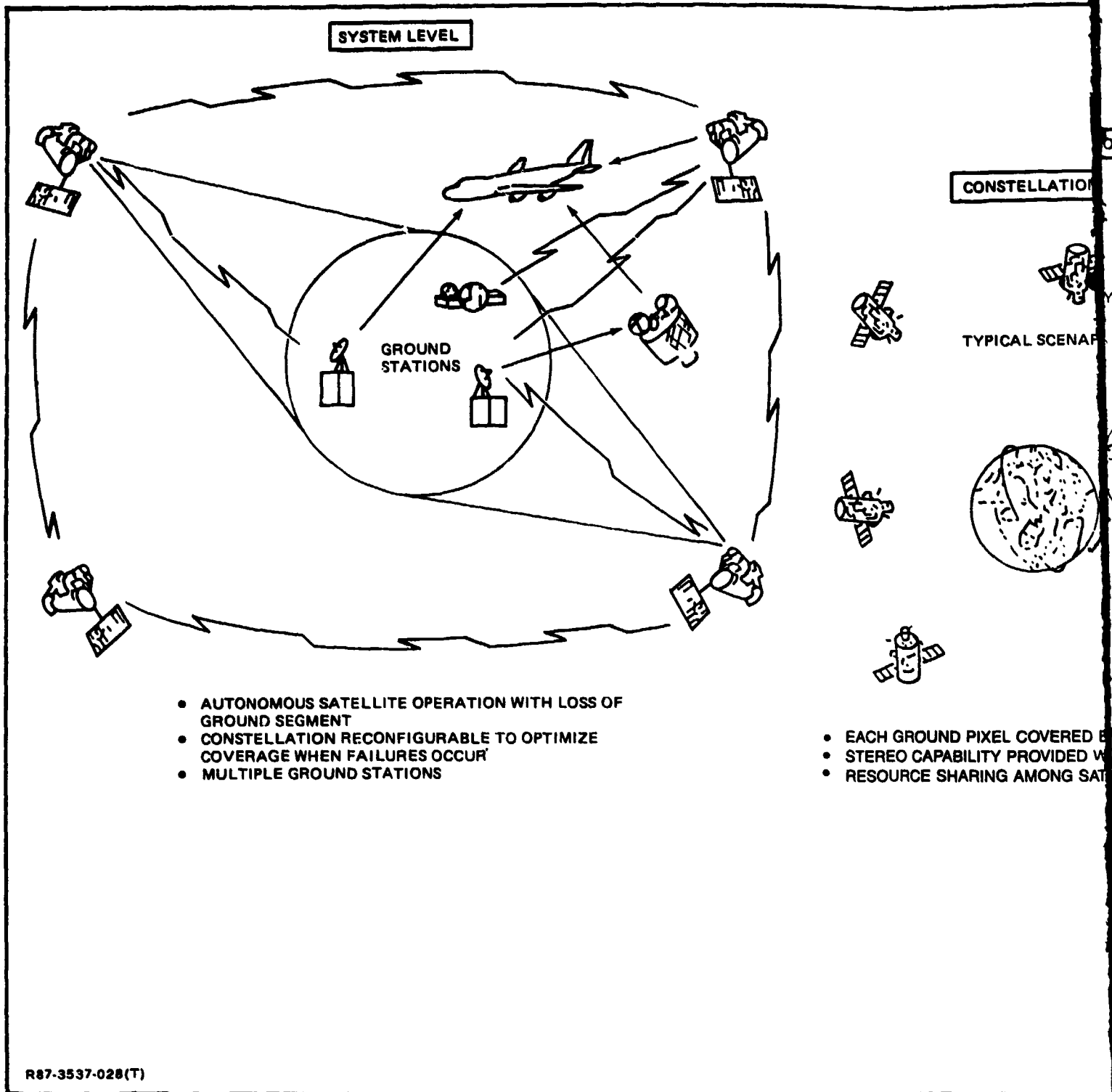
3.2.1 Space Surveillance System

The space surveillance system is responsible for the early detection and tracking of strategic missile launches. This system consists of a constellation of orbiting satellites with IR sensors that detect and track

missile plumes, and a ground segment to process and disseminate the data. As illustrated in Fig. 3-2, fault tolerance is implemented at all levels of the system design.

The fault tolerance approach for the space surveillance system is based on two major considerations: first, the safety concerns associated with the satellite while it is in close proximity to the Shuttle Orbiter; and second, the mission success for the specified life of the satellite. MIL-STD-1574 and NASA publication NHB 1700.7A define the fault tolerance requirements that assure the payload will operate safely during pre-launch, launch and separation from the Shuttle Orbiter. Single fault tolerance is required for critical hazards, while double and triple fault tolerance or inhibits are required for catastrophic hazards. The requirements for mission related fault tolerance are derived from the reliability, global coverage, survivability and availability requirements contained in the system specification. Therefore, the system is designed to tolerate equipment failures during long periods of on-orbit operation and employs a variety of fault tolerance techniques, from error-correcting codes to redundancy of the satellites themselves.

The space surveillance system must provide continuous global coverage even if a satellite fails or is disabled due to an enemy attack. The space segment of the system consists of a constellation containing redundant operating satellites. This extensive fault tolerance approach is appropriate because of the system's high mission criticality and the time delay that would be incurred to launch replacement satellites or to perform on-orbit maintenance. In addition to satellite redundancy, individual satellites have a stringent mission success probability requirement which necessitates the use of extensive fault tolerance. Stringent reliability and fault tolerance requirements are generally considered cost effective for space vehicles because of the high launch and on-orbit repair costs. The program's design goal is that all faults result in either no system degradation or, at worst, degraded performance that would permit ground intervention to restore the system to full performance capability.



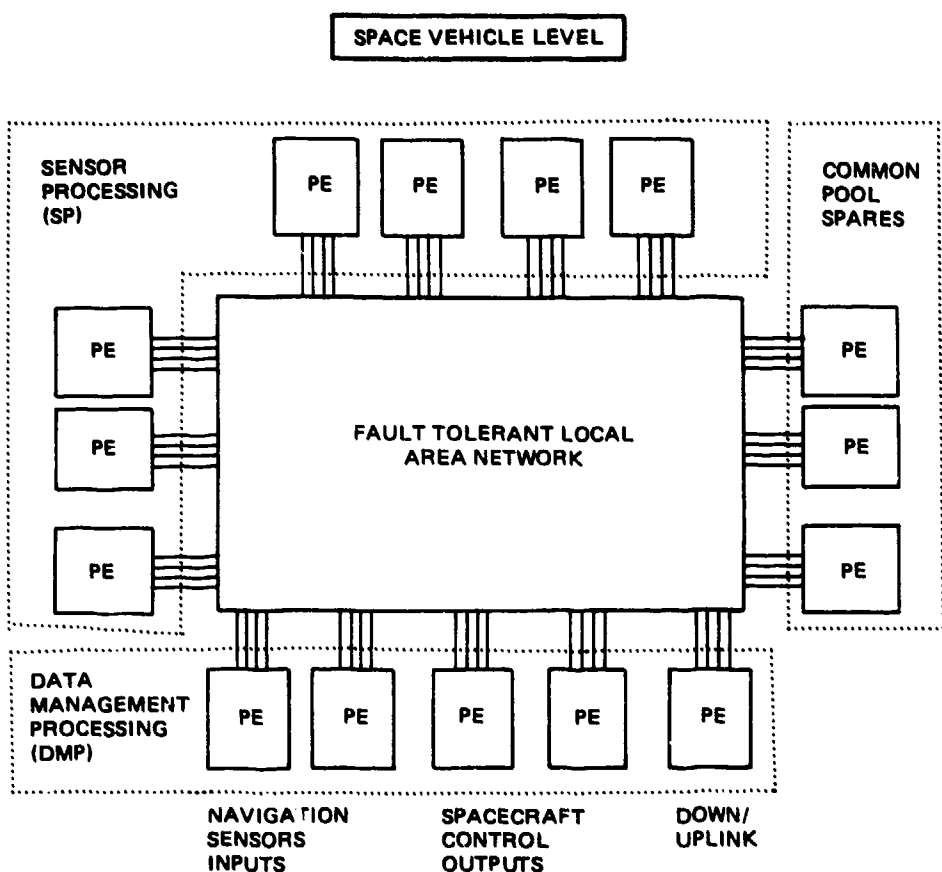
ION LEVEL

NARIO

ED BY 2 OR MORE SATELLITES
ED WITH SATELLITE FAILURE
SATELLITES



SENSOR
INPUTS



- PE - PROCESSING ELEMENT
- LOCAL AREA NETWORK INTERCONNECTS ALL PROCESSING ON SPACE VEHICLE
- LOCAL AREA FAULT TOLERANT NETWORK PROVIDES FOR REPLACEMENT OF FAILED NODE WITH ANY OTHER NODE (I.E., DMP, SP)

Figure 3-2. Space Surveillance System Fault Tolerance.

2

The satellite's mosaic focal plane IR sensor is a highly fault tolerant static sensor containing thousands of mosaic IR detectors. Failures of individual detectors are tolerated since they are masked by the large number of operating detectors and by the data supplied by adjacent satellites viewing the same target area. Although the loss of individual detectors does not compromise system performance, the loss of blocks of detectors would significantly impact the system's detection and tracking capability. Therefore, fault tolerance design guidelines are established to permit only random detector losses. The satellite's IR sensor configuration is similar to the phased array radars which contain numerous transmit/receive modules. Typically between 5 to 10% of these modules can fail randomly before the radar performance degrades beyond its effective use.

The data management subsystem contains the application code that controls the spacecraft subsystems, including the redundancy management functions. Two design goals are established: first, complete fault tolerance for single faults; and second, provide a subsystem similar to a single-string computer, so as to simplify the application code and minimize development cost. The configuration selected consists of a pool of processors from which six are used to form two voting triads. Processing channels in each of the triads communicate with the other elements over interchannel buses. In this manner, data are exchanged for distribution or voting purposes. The hardware automatically handles the protocols required for these data transfers.

If a processor channel fails, that failed channel is removed from operation by the two remaining channels. A new channel is activated, run through self-test, its application code downloaded from mass memory, and synchronization is initiated with the other two operational channels.

The triple modular redundancy (TMR) concept was chosen to meet a stringent time requirement for fault recovery. TMR offered the advan-

tages of a simpler operating system, reduced power consumption, and assurance of single fault tolerance, although the required recovery time could also have been achieved with dual processor pairs having hot backups. Other spacecraft subsystems incorporate similar levels of redundancy and graceful degradation designs to ensure meeting high mission reliability and long mission life requirements.

Fault tolerance requirements for the ground segment are much less stringent than those of the space segment. In general, when a failure is detected, the maintenance personnel can isolate the failure to a line-replaceable unit (LRU), replace the unit with a spare LRU so that the system can resume operations, and repair the faulty unit at one of the ground depot facilities.

For critical command and control functions, a fault tolerant redundant equipment approach is utilized. As an example, if the mission message processor fails in the fixed ground station, the backup support processor will detect the critical condition using a timeout mechanism and then assume the role of the mission message processor. The watchdog timer, shared mass storage, and all mission messages received by both processors, assure a minimum loss of messages to users.

The ground segment operation utilizes fixed and mobile ground stations. Since both stations continuously transmit mission messages to all users, the failure of either station does not result in the loss of transmission capability. Upon failure, a second (backup) mobile station is immediately activated and commences message distribution to restore the multiple source of mission messages. Because of the ready availability of these backup mobile stations, widespread implementation of redundant processors within each station is not cost-effective.

3.2.2 Airborne Surveillance Radar System

In this example, an airborne surveillance radar system will be utilized to illustrate how fault tolerance and in-flight maintenance can be

used to achieve high system availability for long duration missions, and thereby minimize the impact on life cycle cost. The system's operational concept and interfaces are shown in Fig. 3-3. Its primary mission is to locate fixed and moving enemy ground targets and provide near-real-time weapon guidance information to aircraft and missiles. In conjunction with other C³I assets, this system is also used to neutralize enemy forces considered to be an immediate threat. Table 3-1 shows the relative criticality of the various system functions as defined in the system specification. These functional criticalities provided guidance to the contractor in establishing the mission fault tolerance design prioritization. The system specification also listed the acceptable degraded levels of system performance. When coupled with system reliability models (see para. 2.1.1), the functional criticality prioritization was useful in determining whether candidate designs met system reliability requirements. The reliability analysis also considered the effect of added hard-



ware redundancy on overall system reliability and the probability of success for the various functions.

Early in the system's design, RF radiation exposure to personnel, aircraft emergency egress capability and the common safety hazards associated with the operation and maintenance of electronic equipment are identified as the major system safety concerns. These concerns are considered less important in establishing the system fault tolerance requirements when compared to the mission criticality impact. Safety interlocks, overrides and egress features incorporated to assure system safety have a minimal impact on the design configuration and a negligible effect on the acquisition and logistic costs.

In this example, the airborne surveillance radar system is required to operate up to 20 hours in-flight. To achieve high system availability, various forms of fault tolerance are incorporated along with an in-flight maintenance repair capability. In-flight maintenance is accomplished at both the shop replaceable unit (SRU) and LRU levels. The level of in-flight maintenance chosen for each equipment is based on an optimization of on-board spare requirements, diagnostic capability, maintenance personnel workload, and the overall system availability requirement. A one-hour mean repair time is specified for the SRU level and 30 minutes for the LRU level.

The radar antenna of the airborne surveillance radar system is not considered a candidate for in-flight maintenance since it is located externally and is inaccessible during flight. High antenna availability is achieved with the use of fault tolerant design features and with hardware that has proven reliability (where redundancy applications are impractical). The radar antenna aperture contains hundreds of array elements that are electronically controlled to their commanded angle by hundreds of phase shifters (2 elements per shifter).

The radar system performance is highly tolerant to random failures of array elements or phase shifters across the radar aperture. This

characteristic results in gradual, but acceptable, degradation of radar performance and, thus, assures high availability. It permits the establishment of a deferred maintenance approach (i.e., numerous missions can be flown without the need to repair individual array elements or phase shifters until the peak radiated sidelobes degrade beyond their acceptable limits). The array is also mechanically slewed by two servo motors that provide system fault tolerance. In the event that one motor fails to operate, the remaining motor rotates the antenna at reduced slew rates. An inertial measurement unit (IMU) is used to measure the antenna location and is critical to mission success. The IMU is a non-redundant analog device that has demonstrated an excellent field reliability record in similar applications. Alternate redundant design approaches were investigated to increase the fault tolerance of the IMU. It was concluded that the additional hardware complexity made redundancy impractical and not cost effective. Therefore, a decision was made to use a non-redundant IMU configuration and tolerate the infrequent system failures.

The radar transmitters of the airborne radar surveillance system utilize coolanol liquid to safely limit equipment temperatures. Opening coolanol lines in-flight is not recommended from either a maintenance or a safety point-of-view. This precluded the in-flight repair of the transmitters and necessitates a fault tolerant approach for these relatively high failure rate equipments. The configuration selected contains four transmitter units, all of which are required for full mission capability. However, if one or two transmitters should fail, acceptable degraded mission capability still remains although certain enemy targets may not be detectable. Two active radar data processors provide fault tolerance capability. In the event of a processor failure, the operating unit can process all the radar data, but at a reduced data rate.

Other radar equipments are designed to accommodate in-flight repair. The radar control unit, receivers, signal preprocessor, A/D converters and data processors are all essentially non-redundant equipments

that can be easily repaired in-flight. The use of in-flight repair capability, in lieu of equipment redundancy, has the advantages of lower weight, volume and system complexity. This approach must be balanced against the operator workload requirements to optimize the mix of fault tolerance and in-flight repair and minimize LCC while achieving the mission objectives. Diagnostic routines identify the failed SRU or LRU. In most cases, indicator lamps identify the failed hardware. Commonality of replacement modules is stressed throughout the design phase to reduce the number of on-board spares required. Accessibility features are incorporated to permit direct access to each SRU or LRU without prior removal of other components.

3.3 FAULT TOLERANCE REQUIREMENTS CHECKLIST

Air Force and contractor program managers should evaluate the rationale used to establish fault tolerance requirements by using the following checklist:

- a. Are the fault tolerance requirements based on the mission and safety critical functional requirements?
- b. What is the mission criticality (national security, critical, essential, non-essential) of the C³I system? Are the fault tolerance requirements appropriate? (PA)
- c. Does the system have multiple missions with different functional criticalities that require different fault tolerance requirements?
- d. Are the fault tolerance requirements for safety critical functions adequate?
- e. Are the overall fault tolerance requirements too extensive for the system? Can they be reduced to save program cost and reduce the logistic requirements?
- f. Are the fault tolerance requirements consistent with the expected operational use?
 - Is the normal system operation active or standby?
 - What is the intended utilization cycle of the system (8 hours/day, 24 hours/day, continuous, on-demand)?

- What critical system functions warrant continuous monitoring?
 - What system functions are normally active? What system functions are normally passive or operating in a standby mode?
- g. Are the fault tolerance requirements appropriate for the operating environments, i.e., post nuclear blast operation, airborne, spaceborne, ground based, attended, unattended, etc.?

4 - GUIDANCE FOR DESIGN OF FAULT TOLERANCE

Hardware and software redundancy techniques constitute design options that can be selectively employed to satisfy fault tolerant system design objectives. This section provides an overview of many of these techniques and summarizes their advantages, disadvantages and R/M/T impacts. The increasingly important issues of fault detection, distributed processing and the impact of switching are addressed. Reference is made to the *Fault Tolerant Design Implementation Guide* for detailed information pertaining to hardware and software redundancy techniques.

4.1 HARDWARE AND SOFTWARE FAULT TOLERANCE DESIGN OPTIONS

A designer may choose from a variety of fault avoidance and fault tolerance design techniques to satisfy a system reliability or availability requirement. The key elements of fault tolerance and fault avoidance are depicted in Fig. 4-1.

Reliability improvement or fault avoidance techniques in many applications prove to be the least expensive approach to attaining a reliability goal provided they are introduced early in the design process. In a simplex, (non-redundant) system, these techniques are to:

- Obtain higher quality parts/components
- Increase design safety margins/parts derating
- Exercise error-reducing design practice, such as shielding and grounding
- Improve and control the operating environment through cooling, heating and isolation
- Improve user/operator proficiency.

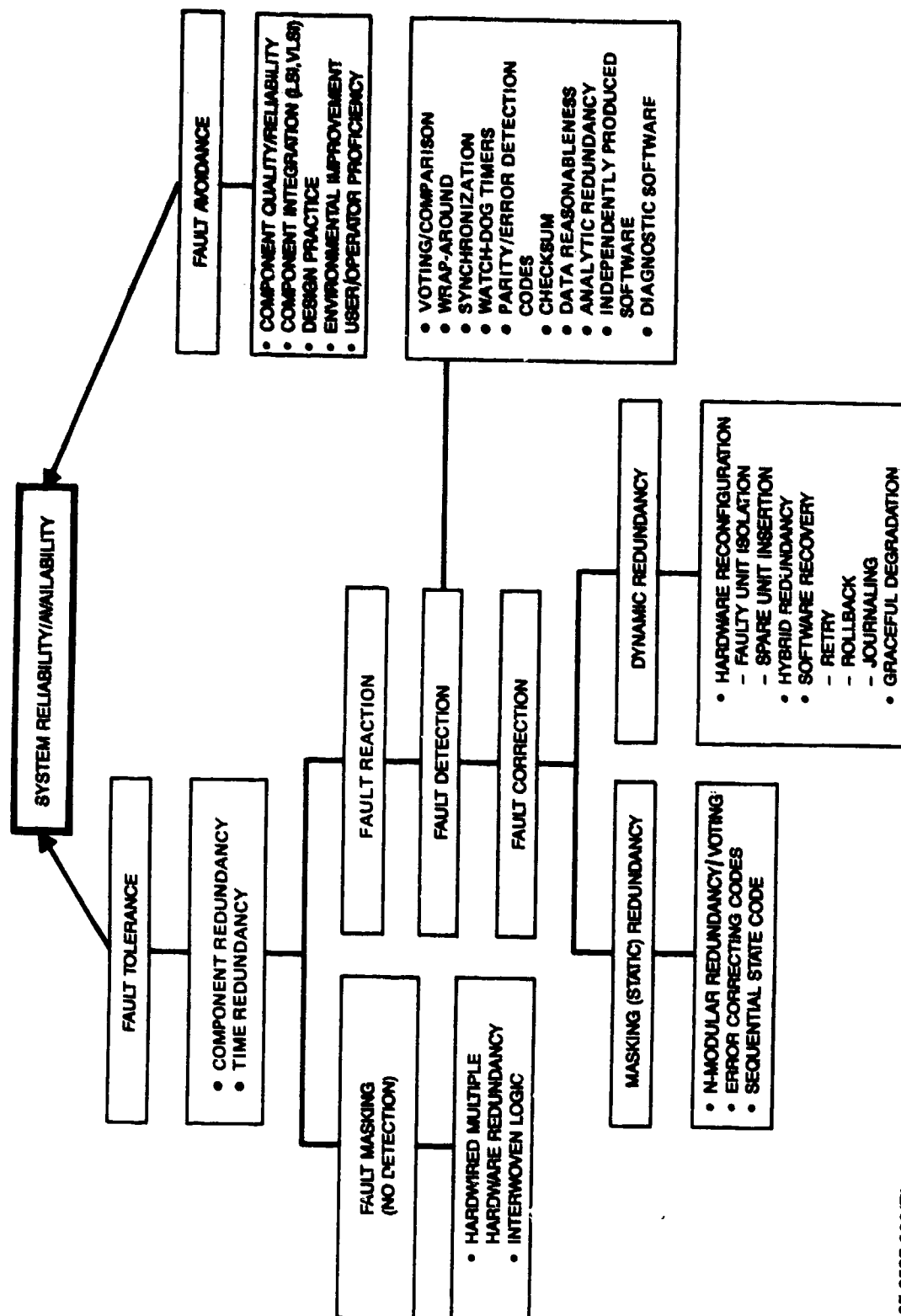


Figure 4-1. Elements of Fault Tolerance.

R87-3537-026(T)

Fault tolerance techniques are applied when the required reliability cannot be obtained with a simplex system. Initially, hardware and software redundancy are incorporated in the system design in order to maintain system operation even if a fault has occurred. This redundancy can take the form of additional hardware components or the use of techniques that serve to delay processing time. Hardware redundancy, the most familiar form, uses on-line, hardwired or off-line components configured either as standby or spare units. Time delay techniques are utilized primarily in software and permit retransmit, recompute, rollback or retry methods of system operation.

In general, fault tolerance design techniques fall into two categories: fault masking and fault reaction. In early applications, fault masking utilized multiple hardware redundancy in either dual, triple or quadruple circuit configurations. In this form, the functional interconnections remained fixed while failures consumed the components until all alternate paths were exhausted. Fault detection was not utilized in conjunction with hardware redundancy, and no intervention was made from outside the circuit to enable switching or reconfiguration. Today, these hardware redundancy techniques are still employed but hardware/software fault masking often utilizes fault detection to initiate system reconfiguration. Switching to standby or spare units is an example of hardware masking, whereas, the use of error detection and correction code is an example of software fault masking.

In all cases, failure detection is the initial step in implementing fault reaction techniques. Detection alone does not provide fault tolerance with continued system operation. The fault must be corrected or the operator informed so an alternate means of operation may be provided. The fault correction techniques or fault reaction "strategies" can be categorized in two forms: masking redundancy or dynamic redundancy. Masking redundancy, in the fault reaction sense, uses both detection

and correction techniques. It is also considered "static" in that it employs built-in hardware for detection, switching, and data error correction and requires no interaction with equipment located outside the subsystem or module. Dynamic redundancy techniques provide reconfiguration of the remaining system elements around the failed element(s). These rely on the ability to fault detect and isolate the failed element(s).

Some of the more commonly used hardware implementations for masking and dynamic redundancy are discussed in paras. 4.1.1 through 4.1.7. Paragraph 4.1.8 discusses failure detection as part of software fault tolerance. Paragraph 4.1.9 presents the characteristics of error detection and correction codes. Paragraph 4.1.10 discusses fault tolerant design implementation in distributed processing systems.

4.1.1 Redundancy Techniques

In reliability engineering, redundancy is the design technique of providing more than one means of accomplishing a given system function; i.e., all paths must fail before the system fails to perform the required function. The alternate means by which the function is accomplished need not be identical to the primary means. Redundancy is implemented to increase the probability of system success where the reliability of a nonredundant design is inadequate to meet the mission or system requirements. The NASA Space Shuttle program is an excellent example of the extensive use of redundancy to achieve program goals. The Shuttle uses four computers which are configured as a redundant set for all critical mission phases, and a fifth computer that contains a backup flight software package and also performs non-critical tasks. The configuration is similar to NMR/simplex with the outputs of the four primary computers voted at the control actuators. Each primary computer monitors the outputs of the four remaining computers, with the redundancy

management circuitry in each primary computer voting to remove the faulty computer from service.

Often, redundancy is implemented to provide fault tolerant designs so that safety requirements can be met. The decision to use redundant design techniques must be contingent on a tradeoff analysis involving mission effectiveness, safety and cost, since additional equipment will increase maintenance expense. Redundancy may be the only available technique after reliability improvement techniques (e.g., derating, design simplification, or substitution with higher quality parts) are shown to be incapable of satisfying program requirements. As an example, incorporating redundant elements may be the best approach for meeting reliability goals for high earth orbit, long-mission-duration satellites for which in-orbit maintenance is not feasible. When on-line maintenance is planned, redundant designs permit repair of failed equipment without loss of system uptime. Because of the increase in system complexity and cost, the use of redundancy with an on-line maintenance concept is normally limited to critical applications.

Redundancy can be incorporated at various assembly levels, as shown by the examples below.

ASSEMBLY LEVEL

EXAMPLES

Part

Micro electronic circuit, transistor, relay contacts.

Circuit

Flip-flops, logic array

Functional

Adders, counters

Subassembly

Arithmetic unit, memory, CPU

Equipment

Computer, gyro, accelerometer

Subsystem

Radar, communications

System

Reconnaissance Spacecraft (constellation)

Incorporating high level active redundancy within VLSI and VHSIC microcircuit chips is a significant advance in the tools available for fault tolerant design. However, common mode failures, such as a hermetic seal failure on a chip, can cause the loss of the entire chips function. Thus, common mode failures become even more significant in system designs when relying on active redundancy within VLSI and VHSIC microcircuit chips. Program managers should require that reliability analyses, such as a failure mode and effects analysis (FMEA), be conducted early in the design process to identify critical failure modes and potential common mode failures. This helps to uncover any potentially serious design problems in a timely manner.

The inherent reliability estimates of the lowest level functional element must be calculated early in the design process. These estimates provide the essential inputs to the reliability models for alternate redundancy configuration candidates. Reliability analysis using these models assists in reducing the number of candidate redundancy schemes capable of satisfying the system reliability requirement. The mathematical models for several redundancy configurations are included in the *Fault Tolerant Design Implementation Guide*.

The penalties associated with the application of redundancy include increased maintenance, weight, space requirements, complexity, cost, spares, and time to design. The increase in complexity results in the increased frequency of unscheduled maintenance. Thus, safety and mission reliability are improved at the expense of components added to the maintenance chain. However, the increase in maintenance may be countered by introducing reliability and maintainability improvement techniques, such as modularity, design simplification, component derating, and the use of more reliable components.

Air Force program managers should insure that the SOW requires the performance and documentation of trade studies when multiple redundancy strategies are being considered. The tradeoff process will help the design engineer determine the most effective redundancy alternative. In the tradeoff process, it may be determined that adding certain types of redundant equipment may impact the cost of preventive maintenance. The cost of this preventive maintenance may become a significant factor in the systems total LCC. Redundancy may be easily implemented if the redundant item is available; may be very feasible if the redundant item is economical when compared to the cost of redesign alternatives; may not be viable if the item is extremely costly or if aircraft/spacecraft weight, volume, or power limitations are exceeded. In any event, the designer should consider all these factors when using redundancy to improve the reliability of critical items (of low reliability) for which a single failure can cause the loss of a system or a major function.

Incorporating redundancy to achieve increased reliability requires an effective fault detection and isolation scheme. Isolation is necessary to prevent failure effects from adversely affecting other parts of a redundant network. For example, failed data processing elements must be isolated, erroneous data must be prevented from contaminating data bases, data base corruption sources must be identified, and provisions must be made to prevent the writing of illegal codes to memory, as well as the writing of legal but incorrect codes to memory. Air Force program managers should ensure that the SOW requires a FMECA be performed at a sufficiently low (detailed) level to uncover any susceptibility of failure propagation in redundant designs.

Testability must be considered when incorporating redundancy into a design. In fact, some circuits may not be checkable prior to mission start because of redundancy inclusion. Without an adequate functional test prior to mission start, it may be possible to determine that only one

of the redundant circuits is functional. In this sense, pre-mission failures could be masked by a redundant item, thus, defeating the purpose of redundancy. Clearly, this is contradictory to the purpose of adding redundancy to improve mission reliability. If it can not be determined that each of the redundant elements is operational prior to mission start, then the design must be questioned. Air Force program managers should insure that the Statement of Work and development specifications adequately address BIT planning and inclusion of test points, etc. when redundancy is anticipated in the system design.


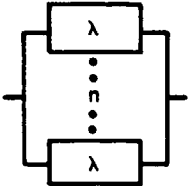
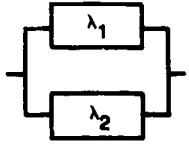
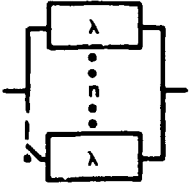
Figure 4-2 presents a summary of several fault tolerant design options with the associated R/M/T impacts and typical applications to current and future C³I systems. Tables 4-1 and 4-2 summarize the characteristics of some fault tolerant design options implemented in software.

4.1.2 Active Redundancy

Active (parallel) redundancy is a design technique where one or more continuously energized redundant elements are added to the basic system so that the function continues to be performed as long as one element remains operative.

Simple active redundancy is configured with identical redundant elements having the same failure rate. Active redundancy configurations also include parallel redundant elements of unequal failure rates as well as series-parallel/parallel-series redundant elements. These and other active redundancy configurations, their corresponding mathematical models, advantages and disadvantages are discussed in Section 7 of MIL-HDBK-338 and in the *Fault Tolerant Design Implementation Guide*.

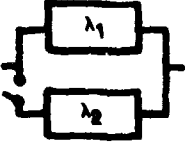
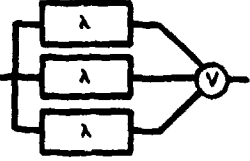
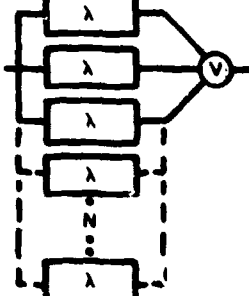
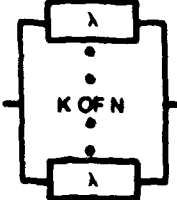
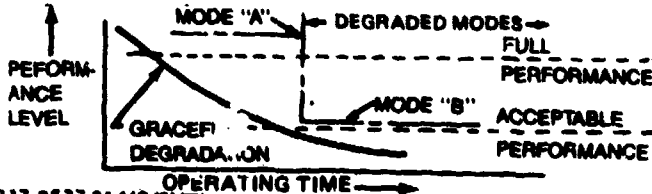
Exercising these mathematical models will establish whether a required probability of mission success within a given operating time can be satisfied through a selective application of active redundancy config-

FAULT TOLERANT DESIGN OPTIONS	RELIABILITY IMPACT	MAINTAINABILITY IM
<p>NON REDUNDANT (SIMPLEX)</p>  <p>EACH AND EVERY UNIT DEPICTED IN THE SERIES CHAIN IS REQUIRED FOR MISSION SUCCESS</p>	<ul style="list-style-type: none"> • UNABLE TO ATTAIN HIGH SYSTEM RELIABILITY FOR SYSTEMS CONTAINING COMPLEX EQUIPMENT OR LONG DURATION OPERATIONS • ACCEPTABLE SYSTEMS RELIABILITY MAY BE ACHIEVED WITH HIGH RELIABILITY EQUIPMENT & SHORT OPERATING TIMES 	<ul style="list-style-type: none"> • MINIMAL SPARES & REQUIRED COMPA SYSTEMS
<p>ACTIVE (SIMILAR) REDUNDANCY</p>  <p>CONSISTS OF A NUMBER (n) OF IDENTICAL, CONTINUOUSLY OPERATING UNITS & ONLY ONE IS REQUIRED FOR MISSION SUCCESS</p>	<ul style="list-style-type: none"> • HIGH SYSTEMS RELIABILITY CAN BE ATTAINED WITHOUT SYSTEMS INTERRUPTION • POTENTIAL COMMON FAILURE MODE (OR THREAT) CAN IMPACT ALL REDUNDANT UNITS 	<ul style="list-style-type: none"> • SEVERE IMPACT OF PERSONNEL SINCE OPERATING CONTI
<p>ACTIVE (DISSIMILAR) REDUNDANCY</p>  <p>CONTINUOUSLY OPERATING UNITS HAVE UNEQUAL FAILURE RATES (λ) & ONLY ONE IS REQUIRED FOR MISSION SUCCESS (SAME AS ACTIVE (SIMILAR) BUT NON-IDENTICAL UNITS UTILIZED)</p>	<ul style="list-style-type: none"> • HIGH SYSTEMS RELIABILITY CAN BE ATTAINED WITHOUT SYSTEMS INTERRUPTION • NORMALLY LESS SUSCEPTIBLE TO COMMON FAILURE MODE OR THREAT ENVIRONMENT 	<ul style="list-style-type: none"> • COMPLICATION OF DIFFERENT UNITS
<p>STANDBY (SIMILAR) REDUNDANCY</p>  <p>CONSISTS OF A SINGLE CONTINUOUSLY OPERATING PRIMARY UNIT, A NUMBER (n) QUIESCIENT IDENTICAL UNIT(s) AND A SWITCH. THE QUIESCIENT/STANDBY UNIT(S) ARE NOT OPERATIONAL UNTIL SWITCHED IN UPON FAILURE OF THE PRIMARY UNIT. ONLY ONE UNIT IS REQUIRED FOR MISSION SUCCESS</p>	<ul style="list-style-type: none"> • VERY HIGH SYSTEMS RELIABILITY CAN BE ACHIEVED COMPARED TO ACTIVE REDUNDANCY IF SYSTEMS INTERRUPT FOR STANDBY UNIT "WARM-UP" & "SWITCH-IN" IS ACCEPTABLE • POTENTIAL COMMON FAILURE MODE OR THREAT CAN IMPACT ALL REDUNDANT UNITS 	<ul style="list-style-type: none"> • MINIMAL SPARES & REQUIRED FOR HI STANDBY UNITS AP LESS LIKELY TO FA

R87-3537-014(1/2)(T)

ABILITY IMPACT	TESTABILITY IMPACT	TYPICAL APPLICATIONS
SPARES & MAINTENANCE PERSONNEL ED COMPARED WITH REDUNDANT S	<ul style="list-style-type: none"> • SELF CHECK CAPABILITY SHOULD BE PROVIDED ON A NON-SYSTEMS INTERRUPT BASIS • LESS COMPLEX FAULT DETECTION/ISOLATION COMPARED TO REDUNDANT SYSTEMS 	<ul style="list-style-type: none"> • LOW CRITICALITY APPLICATIONS OR WHERE REPAIR CAN BE RAPIDLY ACCOMPLISHED TO MINIMIZE DOWNTIME • RELIABLE EQUIPMENT WITH SHORT OPERATING TIME • SYSTEMS WITH CONSTRAINTS IN COST, WEIGHT, VOLUME
IMPACT ON SPARES & MAINTENANCE NEL SINCE ALL UNITS ARE NG CONTINUOUSLY	<ul style="list-style-type: none"> • DIFFICULT TO DETECT A FAULT IN REDUNDANT ELEMENTS WITHOUT A REDUNDANCY MANAGEMENT SCHEME SUCH AS COMPARISON MONITORING, VOTING, ETC. • SELF-TEST CAPABILITY SHOULD BE PROVIDED FOR EACH REDUNDANT ELEMENT 	<ul style="list-style-type: none"> • HIGH CRITICALITY APPLICATIONS WHERE REPAIR CANNOT BE ACCOMPLISHED AND WHERE SYSTEMS OPERATION CANNOT BE INTERRUPTED • COMPUTER PROCESSING, COMMUNICATIONS NETWORKS
ICATION OF SPARING & MAINTENANCE OF NT UNITS	<ul style="list-style-type: none"> • DIFFICULT TO DETECT A FAULT IN REDUNDANT ELEMENTS WITHOUT A REDUNDANCY MANAGEMENT SCHEME SUCH AS COMPARISON MONITORING, VOTING, ETC. • SELF-TEST CAPABILITY SHOULD BE PROVIDED FOR EACH REDUNDANT ELEMENT • ADDITIONAL SOFTWARE TESTING REQUIRED 	<ul style="list-style-type: none"> • HIGH CRITICALITY APPLICATIONS WHERE REPAIR CANNOT BE ACCOMPLISHED OR WHERE SYSTEMS OPERATION CANNOT BE INTERRUPTED • APPLICATIONS WHERE CONCERNS EXIST FOR COMMON MODE FAILURE OR THREAT ENVIRONMENT
SPARES & MAINTENANCE PERSONNEL ED FOR HIGH RELIABLE SYSTEMS SINCE Y UNITS ARE NON OPERATIVE & ARE KELY TO FAIL	<ul style="list-style-type: none"> • DIFFICULT TO DETECT A FAULT IN REDUNDANT ELEMENTS WITHOUT A REDUNDANCY MANAGEMENT SCHEME SUCH AS COMPARISON MONITORING, VOTING, ETC. • SELF-TEST CAPABILITY SHOULD BE PROVIDED FOR EACH REDUNDANT ELEMENT 	<ul style="list-style-type: none"> • HIGH CRITICALITY APPLICATIONS WHERE REPAIR CANNOT BE ACCOMPLISHED & WHERE SYSTEMS INTERRUPT FOR "SWITCH-IN" IS ACCEPTABLE

Figure 4-2. Fault Tolerance Designs Options.
(Sheet 1 of 2)

FAULT TOLERANT DESIGN OPTIONS	RELIABILITY IMPACT	MAINTAINABILITY IMPACT
<p>STANDBY (DISSIMILAR) REDUNDANCY</p>  <p>THE PRIMARY AND STANDBY UNITS ARE DISSIMILAR, HAVING UNEQUAL FAILURE RATES (λ). ONLY ONE UNIT IS REQUIRED FOR MISSION SUCCESS.</p>	<ul style="list-style-type: none"> HIGHER SYSTEMS RELIABILITY CAN BE ACHIEVED COMPARED TO ACTIVE REDUNDANCY WITH SYSTEMS INTERRUPT FOR STANDBY UNIT "WARM-UP" & "SWITCH-IN" NORMALLY LESS SUSCEPTIBLE TO COMMON FAILURE MODE OR THREAT ENVIRONMENT 	<ul style="list-style-type: none"> COMPLICATION OF SPARING OF DIFFERENT UNITS COMPARISON TO SIMILAR STANDBY REDUNDANCY
<p>VOTING REDUNDANCY</p>  <p>ELEMENTS OUTPUT STATE IS DETERMINED BY STATE OF MAJORITY OF INPUTS DETERMINED BY VOTER (V)</p>	<ul style="list-style-type: none"> CAN PROVIDE A SIGNIFICANT GAIN IN SYSTEM RELIABILITY FOR SHORT MISSION DURATIONS POTENTIAL COMMON FAILURE MODE OR THREAT CAN IMPACT ALL REDUNDANT ELEMENTS REQUIRES VOTER RELIABILITY SIGNIFICANTLY BETTER THAN ELEMENT RELIABILITY SYSTEM OPERATION CONTINUES UNINTERRUPTED DUE TO VOTING LOGIC PROVIDING A HIGH CONFIDENCE OF MASKING A SINGLE FAULTY ELEMENT 	<ul style="list-style-type: none"> SEVERE IMPACT ON SPARES MAINTENANCE PERSONNEL. ALL UNITS ARE OPERATING CONTINUOUSLY
<p>HYBRID REDUNDANCY</p>  <p>DEFECTIVE ACTIVE UNIT(S) DETECTED BY VOTER (V) AND REPLACED BY (N) STANDBY SPARE UNIT(S).</p>	<ul style="list-style-type: none"> VERY HIGH RELIABILITY CAN BE ACHIEVED WITHOUT SYSTEMS INTERRUPTION FOR VERY LONG MISSION DURATIONS PROVIDES HIGH CONFIDENCE IN THE CONTINUED ABILITY TO MASK FAULTS BY REPLACING FAULTY "VOTED OUT" UNITS 	<ul style="list-style-type: none"> SEVERE IMPACT ON SPARES PERSONNEL. DUE TO MULTIPLE UNITS OPERATING CONTINUOUSLY IDEAL CONFIGURATION FOR A MAINTENANCE POLICY
<p>K OF N CONFIGURATIONS</p>  <p>OF N IDENTICAL ACTIVE UNITS, K UNITS MUST FUNCTION FOR MISSION SUCCESS (e.g., 2 of 3, 3 of 4, etc.)</p>	<ul style="list-style-type: none"> HIGH RELIABILITY CAN BE ACHIEVED WITHOUT SYSTEMS INTERRUPTION AND WITH MODEST INCREASE IN SYSTEM RESOURCES 	<ul style="list-style-type: none"> SEVERE IMPACT ON SPARES MAINTENANCE PERSONNEL. ALL UNITS ARE CONTINUOUSLY OPERATING
<p>ACCEPTABLE DEGRADED MODES OF OPERATION & GRACEFUL DEGRADATION</p>  <p>PERFORMANCE LEVEL</p> <p>OPERATING TIME</p> <p>MODE "A" DEGRADED MODES</p> <p>MODE "B" ACCEPTABLE PERFORMANCE</p> <p>GRACEFUL DEGRADATION</p> <p>PERFORMANCE</p>	<ul style="list-style-type: none"> NORMALLY, SYSTEMS WITH DEGRADED MODES OR GRACEFUL DEGRADATION CAN ACHIEVE HIGH RELIABILITY LEVELS WITH MINIMAL INCREASES IN HARDWARE RESOURCES 	<ul style="list-style-type: none"> MINIMAL SPARES & MAINTENANCE PERSONNEL REQUIRED FOR HIGH SYSTEMS COMPARED WITH OTHER REDUNDANCY TECHNIQUES IDEAL CONFIGURATION FOR A MAINTENANCE POLICY

R17-3537-014(2/2)(T)

IMPACT	TESTABILITY IMPACT	TYPICAL APPLICATIONS
OF SPARING & MAINTENANCE UNITS COMPARED WITH BY REDUNDANCY	<ul style="list-style-type: none"> SELF-TEST CAPABILITY SHOULD BE PROVIDED FOR EACH REDUNDANT ELEMENT 	<ul style="list-style-type: none"> HIGH CRITICALITY APPLICATIONS WHERE REPAIR CANNOT BE ACCOMPLISHED & WHERE SYSTEMS INTERRUPT FOR "SWITCH-IN" IS ACCEPTABLE APPLICATIONS WHERE CONCERNS EXIST FOR COMMON MODE FAILURES OR THREAT ENVIRONMENT
ON SPARES & PERSONNEL SINCE OPERATING Y	<ul style="list-style-type: none"> SELF-TEST CAPABILITY SHOULD BE PROVIDED FOR EACH REDUNDANT ELEMENT 	<ul style="list-style-type: none"> HIGH CRITICALITY APPLICATIONS WHERE REPAIR CANNOT BE ACCOMPLISHED AND WHERE SYSTEMS OPERATION CANNOT BE INTERRUPTED
ON SPARES & MAINTENANCE UE TO MULTIPLE ACTIVE UNITS URATION FOR A DEFERRED POLICY	<ul style="list-style-type: none"> DIFFICULT TO DETECT A LATENT FAULT IN REDUNDANT ELEMENTS WITHOUT A REDUNDANCY MANAGEMENT SCHEME SELF-TEST CAPABILITY SHOULD BE PROVIDED FOR EACH REDUNDANT ELEMENT 	<ul style="list-style-type: none"> HIGH CRITICALITY APPLICATIONS NORMALLY OF LONG MISSION DURATION WHERE HIGH CONFIDENCE IN THE ABILITY TO MASK FAULTY OUTPUTS IS ESSENTIAL
ON SPARES & PERSONNEL SINCE ALL UNITS OUSLY OPERATING	<ul style="list-style-type: none"> DIFFICULT TO DETECT A FAULT IN REDUNDANT ELEMENTS WITHOUT A REDUNDANCY MANAGEMENT SCHEME SUCH AS COMPARISON MONITORING, ETC. SELF-TEST CAPABILITY SHOULD BE PROVIDED FOR EACH REDUNDANT ELEMENT 	<ul style="list-style-type: none"> HIGH CRITICALITY APPLICATIONS WHERE REPAIR CANNOT BE ACCOMPLISHED AND WHERE SYSTEM OPERATION CANNOT BE INTERRUPTED
ES & MAINTENANCE EQUIRED FOR HIGH RELIABLE PARED WITH OTHER TECHNIQUES URATION FOR A DEFERRED POLICY	<ul style="list-style-type: none"> SYSTEM SHOULD BE DESIGNED TO DETECT A THRESHOLD ABOVE THE MINIMUM ACCPETABLE PERFORMANCE LEVEL 	<ul style="list-style-type: none"> RESTRICTED TO THOSE TECHNICAL AREAS WHERE THIS APPROACH IS APPLICABLE, I.E., PHASED ARRAY RADARS, SOLAR ARRAYS, I.R. SENSORS, ETC.

Figure 4-2. Fault Tolerance Designs Options.
(Sheet 2 of 2)

4-11/12

TABLE 4-1. Detection Technique Characteristics.

DETECTION TECHNIQUE	APPLICATION	IMPLEMENTATION LEVEL	ISOLATION CAPABILITY	RESPONSIVENESS	COMPLEXITY
VOTING/COMPARISON	ANALOG ELEMENTS, DIGITAL LOGIC	MODULE, FUNCTION, UNIT	FINE-TO-COARSE	HIGH	LOW TO MEDIUM
WRAP-AROUND	ANALOG AND DIGITAL ELEMENTS	MODULE, FUNCTION	FINE-TO-MEDIUM	MEDIUM	LOW TO MEDIUM
PARITY	DIGITAL TRANSMISSION AND STORAGE	DIGITAL WORD	FINE	HIGH	LOW
CHECKSUM	DIGITAL TRANSMISSION AND STORAGE	DIGITAL WORD BLOCK	COARSE	HIGH	LOW
ERROR DETECTION CODES	DIGITAL TRANSMISSION	DIGITAL WORD	FINE	MEDIUM	MEDIUM
SYNCHRONIZATION	DIGITAL PROCESSES	FUNCTION	COARSE	LOW	MEDIUM TO HIGH
WATCH-DOG TIMER	DIGITAL PROCESSES	FUNCTION	COARSE	LOW	LOW
DATA REASONABLENESS	ANALOG OR DIGITAL PROCESSES	FUNCTION	MEDIUM	HIGH	MEDIUM
ANALYTIC REDUNDANCY	ANALOG ELEMENTS OR PROCESSES	FUNCTION, UNIT	MEDIUM	MEDIUM	MEDIUM TO HIGH
DIAGNOSTIC SOFTWARE	DIGITAL PROCESSES	MODULE, FUNCTION, UNIT	FINE TO MEDIUM	LOW	HIGH
INDEPENDENTLY-PRODUCED SOFTWARE	DIGITAL PROCESSES	MODULE, FUNCTION, UNIT	MEDIUM TO COARSE	LOW	HIGH
TOTALLY SELF CHECKING/FAULT SECURE NETWORKS	DIGITAL PROCESSES	DIGITAL WORD	FINE	HIGH	MEDIUM

R87-3537-012(T)

TABLE 4-2. Properties of Error Detection Codes.

CODE TYPE	CAPABILITIES		COMPLEXITY
	DETECTION	CORRECTION	
PARITY	ANY SINGLE-BIT ERROR. NO DOUBLE-BIT ERRORS SOME MULTIPLE, ADJACENT, UNI-DIRECTIONAL ERRORS	NONE	LOW
HAMMING	ANY SINGLE-BIT ERROR ANY DOUBLE-BIT ERROR	SINGLE BIT	HIGH
M-OF-N	ANY SINGLE-BIT ERROR 1-OF-3 DOUBLE-BIT ERRORS ANY MULTIPLE ADJACENT UNI-DIRECTIONAL ERRORS	NONE	MEDIUM
AN	ANY SINGLE-BIT ERROR	SINGLE BIT	LOW
RESIDUE-M	ANY SINGLE-BIT ERROR	SINGLE BIT	MEDIUM
CYCLIC	SINGLE-BIT TO MULTIPLE, RANDOM BITS. BURST ERRORS.	SINGLE AND RANDOM MULTIPLE SINGLE BURST	MEDIUM TO HIGH

R87-3537-013(T)

urations. These configurations often differ in weight, volume, power, cost as well as in maintenance frequency, maintainability and testability.

Therefore, AF program managers should insure that the SOW requires the development of accurate reliability models so that comparisons and tradeoffs between alternate hardware architectures and redundancy schemes may be accomplished.

4.1.3 Standby Redundancy

Standby redundancy is a design technique where an alternate redundant means of performing the function is switched in when it is determined that a failure has occurred in the primary element performing the function. This differs from active redundancy in that the redundant unit(s) (or elements) are not operating until switched into the system as a substitute for the failed primary unit. Switching, therefore, is always required to activate standby redundant units.

Standby elements are less susceptible to failure since they are not operating until switched in. Therefore, when compared to active redundancy, higher systems reliability can be achieved if system complexity and systems interrupt due to warm-up and switching time penalties are acceptable. Although, only one redundant element is required to operate in the system for mission success, self-test capability is necessary for all elements to assure fault detection capability.

Standby redundancy may be implemented at various assembly levels, (e.g., part, circuit, functional, sub-assembly, equipment, subsystem and system). However, the implementation level chosen depends to a great degree on an analysis of the switch complexity and the tradeoff conclusion. In addition to maintenance cost increases for repair of the additional standby elements, the system probability of success of certain

standby redundant configurations may actually be less than that of a single element. This results from the impact of the reliability of switching or other peripheral devices needed to switch-in the standby redundant element(s). Care must be exercised to ensure that reliability gains are not offset by increased failure rates due to switching devices, error detectors and other peripheral devices needed to implement the standby redundancy configurations.

The effectiveness of standby redundant configurations is enhanced since this configuration allows repair of the failed unit (while operation with the good unit continues). Through continuous or comparative monitoring, the switchover function can provide an indication that a failure has occurred and operation continues with the alternate unit. With a positive failure indication, delays in repair can be minimized. Ground-based and large airborne weapons systems, such as AWACS and Joint STARS, are examples of systems that utilize on-line repair techniques to enhance availability.

4.1.4 Voting Redundancy

Voting redundancy is a design technique in which the element's output state is determined by a voter or comparator that compares or analyzes the state of the majority of the inputs. Faults are statically masked in voting redundancy, since the agreeing outputs are selected by the voter and the faulty outputs are ignored. Thus, the majority of agreeing outputs (presumed to be good) allows continuation of the elements intended function without interruption. Voting redundancy must be configured with an odd number of elements to avoid the possibility of tie-vote ambiguity. Minimum element implementation, called triple modular redundancy (TMR), outputs the result of two or more of three agreeing outputs by its voter. A more general implementation, N-modular redundancy (NMR), outputs the majority of N element outputs that agree. Voting may be applied to analog and digital signals and is commonly applied at the module level.

The penalty associated with N-modular redundancy includes the complexity (N) times the basic hardware complexity (cost, weight and power), plus the complexity of the voter. The voter may also cause a signal propagation delay leading to a decrease in performance. To achieve the reliability potential of NMR configurations it is important to prevent the voter from becoming a single point failure. This can be overcome by introducing one or more redundancy techniques into the voter design.

4.1.5 Hybrid Redundancy

Hybrid redundancy is a dynamic redundancy technique in which failed NMR modules (see para. 4.1.4) are replaced with previously unused spare modules. When the voter detects a disagreement in a hybrid redundant system, the module or modules in the minority are considered to be failed and are replaced by an equivalent number of spare modules. Thus, a fault occurring in a TMR configuration results in the triad being reconfigured back to a state where it can once again mask faults. Hybrid redundancy overcomes one of the drawbacks of NMR since the fault masking capability of an NMR design degrades rapidly as elements fail and the possibility exists for a collection of failed elements to out-vote the remaining healthy elements, thereby leading to premature system failure. Thus, hybrid redundancy is a design solution to meet stringent system reliability requirements of uninterrupted performance where the mission duration is very long and maintenance is not possible.

The spare modules used in hybrid redundancy often are described as pooled spares (i.e., they are not dedicated to any particular module but can replace any module when called upon). Depending on the application, the pooled spares can be cold, hot, or flexed.

Cold spares do not operate until they are switched in. Therefore, they will exhibit a lower failure rate than pooled spares that are powered (hot). Consequently, using cold pooled spares in a hybrid redundancy configuration results in higher system reliability than can be obtained by

using hot spares. This approach often provides significant advantages in situations of long duration missions without maintenance (e.g., satellite applications). It may also result in fewer spares, lower power requirements, and reduced weight over a hot sparing strategy.

Hot pooled spares are modules or equipment that are powered and operating in a slave mode. These may be shadowing the operating elements of the NMR core, but their output is not being voted upon. Thus, delay time (to reconfigure) is minimized. The advantage of a hot standby architecture (to mask failures) is that takeover by the slave is virtually instantaneous. The slave needs no updates because it is doing the same tasks as the master NMR core elements. Disadvantages of using hot pooled spares are increased probability of failure during long duration missions and increased power and weight required for a given allocated system reliability. In many applications of hybrid redundancy, hot standby spares may be inefficient and may waste resources, since the spares are dedicated exclusively to the functions of the NMR core. However, where the penalty of failure is extreme, such as those affecting national security, this type of redundancy may be appropriate.

Flexed spares are spare elements of a system which are exercised periodically and systematically. The use of flexed spares reduces the possibility of a cold spare not working during a reconfiguration attempt. For maximum effectiveness and confidence, this strategy requires that spare buses, modules, voters, power supplies and clocks be periodically tested during the mission.

4.1.6 K of N Configurations

A K out of N configuration is a system consisting of N elements, of which at least K elements must be functioning in order to achieve system mission success. All N elements in the configuration are operating in parallel, similar to the operation of a system configured in active parallel redundancy (see para. 4.1.2). However, instead of requiring only one

of the N elements to function (as in active parallel redundancy), all K elements must function to attain system mission success. Examples of K out of N configurations are:

- Spacecraft attitude control thruster engines
- Inertial reference assemblies
- Triple modular redundancy (TMR).

In the first example above, a spacecraft may be designed such that its attitude control is maintained with any of 8 (or more) of 16 thrusters functioning. The second example is an integrated inertial reference assembly designed so that any 3 or more of 6 gyros and any 2 or more of 4 operational accelerometers will produce an accurate inertial reference function. Last is an example of triple modular redundancy (see para. 4.1.4) in which any two or more of the three elements must function (agree) in order for the system to function successfully.

4.1.7 Graceful Degradation

Graceful degradation is a design technique which utilizes extra hardware as part of the system's normal operating resources to ensure, with high probability of success, that an acceptable (minimum) performance level can be maintained in the presence of failures. Therefore, the extra hardware may raise system performance above minimum requirements; this enhanced performance continues as long as the extra hardware is not required to overcome failure effects. Potential failure modes that cause only a partial loss of functional capability may require lower levels of fault tolerance, thereby reducing hardware complexity and the overall system cost. The extra hardware used in gracefully degrading systems differs from standby redundant and hybrid redundant configurations in that the extra hardware contributes to normal system performance and does not have to be switched in.

Two examples of gracefully degrading systems are large C³I phased-array radar systems and distributed processing systems. A phased-array radar antenna typically contains a large number of transmitting and receiving elements. A small number (typically less than 5%)

of randomly dispersed failures of these elements has a negligible effect on system performance, and additional failures can be compensated for by boosting transmitter power or receiver gain. An even larger number (typically less than 10%) of random element failures might be offset by the capability of the surviving elements to meet minimum acceptable system performance requirements with a degraded detection capability as illustrated in Figs. 4-2 and 4-3. These antennas are adaptable to a deferred maintenance policy wherein failed elements need not be repaired after each mission. A second example of graceful degradation is a distributed data processor subsystem in which the network contains extra operating processors that provide additional throughput. If any processor

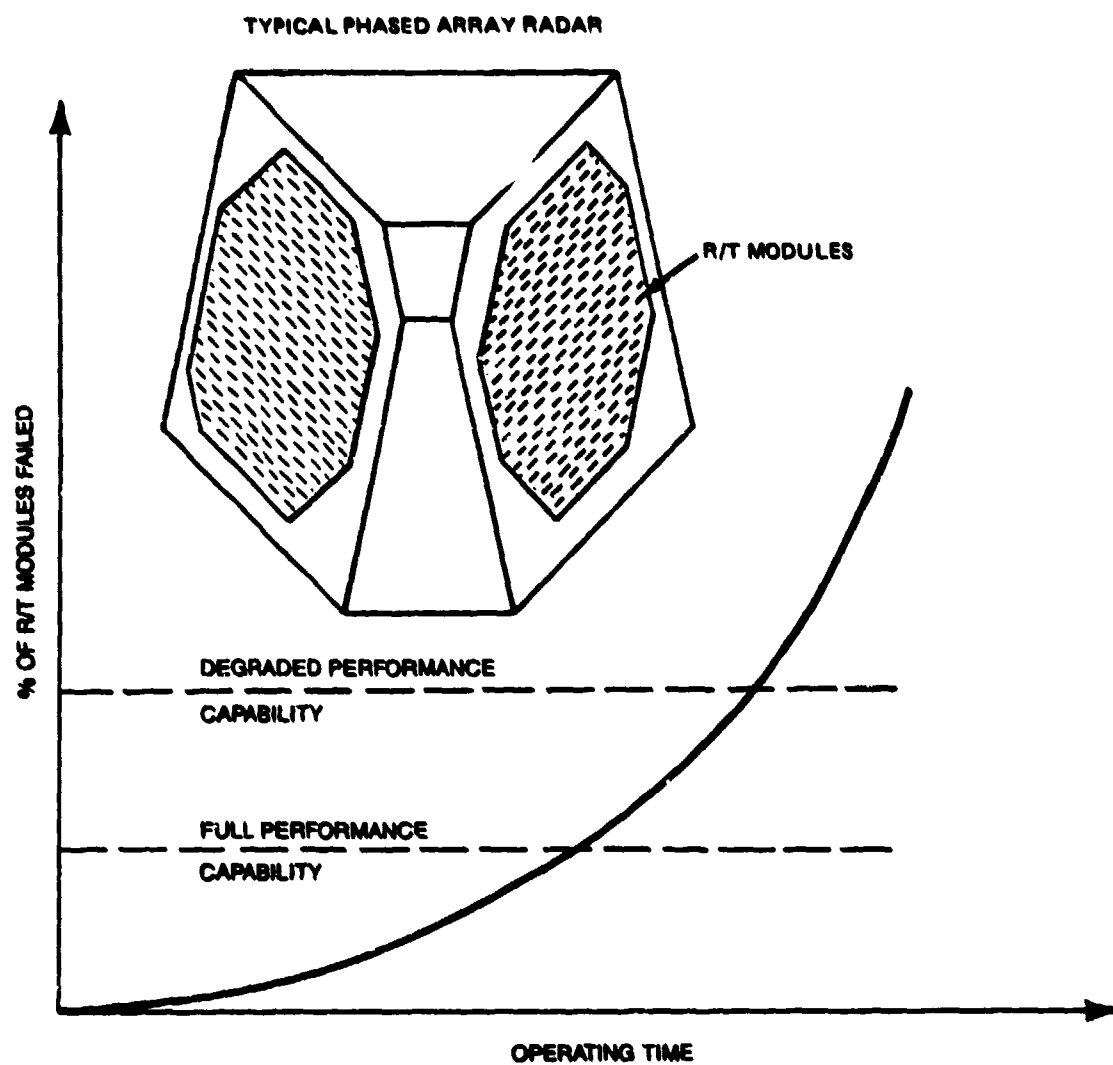


Figure 4-3. Graceful Degradation of Antenna Receive/Transmit (R/T) Modules.

fails, only the excess capacity is lost. The number of extra processors to be included in the network can be selected to yield an allocated probability of maintaining at least minimal system functionality through the end of the mission.

Graceful degradation implies that element failures are unlikely to cause extensive secondary failures. Limiting secondary failures, i.e., fault containment, may require careful design of the interconnection between adjacent and groups of adjacent phased array radar elements. Also, the data output of a failed data processor must be prevented from contaminating other operating elements. The AF program manager should ensure that the SOW and CDRL require that an FMEA be performed at a functional or hardware level to indicate the consequences of element failure(s) in a gracefully degrading system. The purpose of carefully selecting the level of detail in the FMEA is to highlight the susceptibility of the design to data contamination or secondary failure(s) so that corrective redesign may be instituted.

4.1.8 Fault Detection Techniques

Many methods are available to detect hardware failures and data errors. Most have been conceived to satisfy the goals of specific system types such as analog control, communications, and processing systems. The different techniques used provide varying levels of three primary characteristics:

- *Responsiveness* - Time to detect
- *Failure Source Isolation Level* - Component, module, function or system unit
- *Implementation Complexity* - Directly related to the cost to incorporate.

Most highly fault tolerant systems use a combination of techniques. Table 4-1 lists the common methods which include detection approaches for both hardware and software intensive systems. The choice of a specific detection technique depends upon the nature and criticality of the element or task. The cost and complexity of implementing it must be assessed along with the accuracy of the method used.

4.1.9 Error Detection Codes

Systematic coding of transmitted data is the method most often used to detect errors that occur in digital communication. Errors can occur singly, in multiples of random errors, or in bursts due to timing inconsistencies or noise caused by electromagnetic interference. Distinct classes of codes have been configured to deal with the various types of errors expected. The more complex error patterns demand the use of more sophisticated error detection coding techniques. In addition, the advanced detection techniques can be enlarged and designed to correct the errors; thus, they provide a form of masking redundancy. All codes apply data redundancy to an information stream that is predetermined and consistent. Error correction is often incorporated in these designs. The complexity and the detection/correction capabilities of some commonly used code types are summarized in Table 4-2.

4.1.10 Distributed Processing

Distributed processing allows for computational functions to be dispersed among several physical computing resources. The resources may be geographically separated or co-located. Computations are performed locally but the processors may be linked to permit separate tasks to be partitioned between computational resources. Three important aspects of distributed processing systems are the design of the local computational resources, the network which allows the processors to communicate with one another and the operating system used to allocate the partitioning of the tasks to the local processing elements.

Distributed processing systems are one of the most implementable design techniques for fault tolerant designs. The various fault tolerant hardware and software techniques identified in this Guide can be applied to the local computational resources. The network requires forms of message checking and redundant communication paths. The operating system, critical to the success of the system should generally be distributed and redundant to minimize the impact of a failed memory module storing the program.

Distributed Processing offers many advantages over other processing systems including the centralized approach. These advantages include the following characteristics:

- extendability,
- fault tolerance, and
- implementation attributes.

Extendability, sometimes referred to as modularity, flexibility or adaptability is the degree to which system functionality and performance can be changed without changing the system design. The major benefits of extendability are ease of growth and ease of modification. A high degree of extendability permits performance upgrades in small increments at correspondingly small cost increases. Reduced hardware and software development and support costs will be achieved by commonality of system elements such as nodal data processors and bus control units. Distributed processing systems' fault tolerance is enhanced by the multiplicity of independent processors which may improve fault detection, isolation and recovery through cooperation of the processors. Graceful degradation is easily implemented in distributed processing systems, since the loss of a single processor may only result in a slight incremental decrease in performance or throughput. Errors occurring in a single processor are confined and only a subset of system functionality and performance may be affected. Furthermore, spare redundant processors may easily be connected to the network to facilitate meeting a stringent reliability/availability requirement. The application characteristics of distributed processing systems are concerned with attributes such as bandwidth, maturity and technology insertion. The system response time and throughput are both improved by a multiplicity of processors operating concurrently. There are also several cost-effectiveness advantages for using an aggregate of interconnected smaller processors instead of more traditional-centralized systems of equivalent performance. First, the quantity and functionality of the smaller processor's logic is more amenable to high levels of semiconductor integration than is that of the larger processor. Second, smaller processors can be designed and implemented more quickly, so they can make use of the lat-

est, most cost-effective hardware technology. Finally, smaller processors are manufactured in greater quantities and thus benefit from production economies.

However, there are limitations and design issues associated with distributed processing systems. These include:

- The amount of internal processing contained in a node must be traded in the design phase against the addition of more computational nodes.
- The nodes in a network can be interconnected in many ways (fully connected, multiply connected, star, ring, tree, etc.) and these must be traded in the design phase against connectivity and reliability goals.
- The bandwidth requirements for the network are driven by the number of messages and associated protocol. The bandwidth in turn dictates the technology used in the implementation. Inadequate bandwidth will degrade the response time of the system.
- A fully distributed system carries a substantial amount of overhead particularly in the operating system. It is the responsibility of the operating system to schedule tasks to the computer resources and to determine their health status. A failed computer resource must be taken off line and its tasks reallocated by the operating system to a healthy processing unit. The amount of time allowed for reconfiguration is driven by the system requirements, the complexity of the operating system, and the technology proposed for the distributed system.
- The data base operating system concerns can become complex when other processing resources require a non-resident data base; for example, in extracting data which is not local to the processing resource.

Failure to address the above design issues in a timely manner can result in excessively long response times, poor reliability and increased system costs. When a C³I systems development effort includes a selection

between centralized and distributed processing system approaches, it is important that this selection be made no later than the end of the Demonstration/Validation phase. There are significant complexity, systems integration, and development effort considerations associated with distributed processing systems. Therefore, contractor program managers should identify and schedule appropriate trade studies and analyses to support the recommended data processing approach.

Distributed processing systems are gaining increased importance in satisfying C³I system development objectives. They can be designed to contain a wide range of hardware and software fault tolerance techniques and thus satisfy stringent long life, autonomous operation and availability requirements. Further information including R/M/T impacts of various distributed processing architectures is provided in the *Fault Tolerant Design Implementation Guide*.

4.1.11 HARDWARE AND SOFTWARE FAULT TOLERANT DESIGN

CHECKLIST QUESTIONS

The following questions will provide guidance for AF program managers and contractor designers during the development of system architectures for fault tolerant C³I systems.

- a. What system requirement has driven the decision to incorporate redundancy? (C)
- b. Has the decision to incorporate redundancy techniques been based upon a tradeoff analysis?
- c. Have the cost benefits of other reliability improvement techniques (e.g. parts derating, design simplification, environmental stress screening, etc.) been considered prior to the decision to duplicate hardware/software?
- d. What alternate redundancy technique(s) have been identified which satisfy the allocated reliability requirement? Do these alternates result in lower system weight or cost?

- e. Has the designer considered the added complexity, cost, and weight of fault detection, isolation, switching, and other peripheral devices needed to implement the particular redundancy configuration? (C)
- f. Have the levels of implementation of redundancy been selected with testability considerations in mind?
- g. Has the reliability and availability of the system been accurately modeled at the level of implementation of redundancy?
- h. Has the switch failure rate been incorporated in the reliability model of standby and hybrid redundancy?
- i. Has the voter/comparator failure rate been incorporated in the reliability model of voting redundancy configurations? What means have been taken to prevent the voter from becoming a single point failure?
- j. Have the following approaches been considered when pooled spares are to be employed in mission and safety critical applications? (C)
 - design soft turn-on circuitry for cold spares
 - operate with standby spares
 - operate with flexing of spares.
- k. Is the distributed processing operating system redundant so as to minimize the impact of a failed memory module?
- l. Does the operating system periodically check the health status of spare redundant modules?

4.2 MAINTAINABILITY/TESTABILITY IMPACT ON FAULT TOLERANT DESIGN OPTIONS

4.2.1 Testability of Fault Tolerant Designs

The success of most fault tolerant systems depends largely on the design's inherent diagnostic capability and testability--specifically its ability to detect, identify, and report malfunctions so that suitable corrective action can be taken. The selection of a redundant design technique must include an assessment of associated diagnostic/testability alternatives and their overall impact on the achievement of the design

goal performance requirements. The methods chosen to implement the diagnostic/testability task depend on what is being tested with the fault tolerance design option. Once a method is chosen, constraints imposed upon it begin to reveal themselves from various other interdependent requirements. Design for pure testability, whether in a fault-tolerant framework or not, can be realized only after the designer has dealt with constraints such as cost, available real estate, size and weight limitations, available power, and interface complexity restrictions.

When performing trades to secure additional real estate or complexity for diagnostic/testability capability for fault tolerant systems, the designer has more freedom than the designers of conventional systems. This is because the added hardware and software for the test function serve multiple purposes: First, performance-monitoring testing assures the user that the equipment is working. Secondly, this testing capability helps to isolate faults to a replaceable module. Thirdly, in standby redundant strategies, the built-in self-test or diagnostic function must detect and identify malfunctions so that the standby or redundant function can be switched in. This third functional requirement demands that designers be more responsive to the diagnostic/testability needs. By integrating all three diagnostic capabilities into a cohesive concept, the overall task can be accomplished much more easily.

One of the most demanding requirements imposed on the diagnostic/testability capability of fault tolerant system design is a quick response time to reconfigure. Systems with no critical reconfiguration response times are free to have self-test diagnostics put into a low priority background mode. These systems need not compete for processing time, serial bus access, or slow electro-mechanical relay switching time, to mention just a few examples.

Additional hardware and/or software may be required to internally test a function such as a self-test diagnostic capability. This addition may be beyond what is necessary to perform its normal dedicated function. As a general rule, contractor program managers should establish a goal

that the test circuitry to be added has a failure rate an order of magnitude better than the functional circuitry to be tested. This goal may be relaxed if the program manager is satisfied that it is too stringent and would compromise the ability to satisfy other critical system design requirements. Air Force program managers should assure themselves that the ratio of BIT circuitry failure rate to functional circuitry failure rate is not excessive. This will minimize corrective maintenance events due to failures of an overly complex BIT diagnostic function. However, there should be sufficient diagnostic capability built into the design to reliably carry out these detection, identification and reporting test functions.

An important factor influencing the diagnostic/testability design is new technology. Today, more can be accomplished with a package of the same size as that of 10 years ago. However, there is a tendency to shy away from new technology because of lack of confidence resulting from insufficient field testing. Risks associated with single-source procurement have been used as a possible reason to reject a good solution. Therefore, although determining how to test a function may be readily resolved by using a new technique, alternate solutions are often sought because of lack of confidence in the new technique.

System reliability can be improved by using redundancy techniques, but caution must be exercised in this approach. Fault detection and isolation are often the limiting factors when designing redundancy into the system. For example, a subsystem may consist of a number of redundantly configured items and the reconfiguration strategy may require isolating a failed item before an operationally redundant item can be switched into its place. Depending upon function criticality, redundant units can be switched in either at the first indication of a failure or after a failure indication has been sustained. In either case, after the spare unit has been switched in, the operating system can command more exhaustive BIT on the faulty module and log the unit as failed if confirmed by BIT, or return the unit to standby or active status if the fail-

ure is not confirmed. When considering adding more redundant items, caution is required since the diagnostic/testability of failed items is seldom 100% perfect. When the non-perfect probabilities of correct failure detection and isolation are taken into account, it is entirely possible that the subsystem probability of mission success may not increase with the addition of redundant items.

It may be helpful to review some of the more desirable design considerations for diagnostics/testability before establishing what can be expected from the diagnostic design of a fault tolerant system. These design considerations include the following:

- a. *Comparison Method* - An effective method for testing similar systems with similar inputs and outputs is to compare outputs and flag any gross disagreements. It is desirable to provide a means to determine which branch is faulted.
- b. *Redundancy Verification* - The built-in test should test each redundant path individually whenever possible, to prevent the masking of faults in redundant items.
- c. *Flexing of Spares* - Periodically activate all available assets when continuous or concurrent fault detection methods are utilized within hot spares, so that the built-in test of the hot spares is activated and reported out before these items are needed and switched in.
- d. *Voting Scheme Technique* - A typical example of a voting scheme technique is to compare output values from three different sources. Confidence is placed in that value where at least two of the three sources agree. The source of the erroneous value should be corrected at an appropriate maintenance schedule.
- e. *Error Correction* - Detection of degraded performance in stages preceding an error-correcting function is difficult. This is be-

cause the error-correcting function makes its preceding degraded stage appear healthy. The error-correcting functions should keep a count of the number of times corrections had to be made. When a predetermined threshold count is exceeded, a test signal may be injected to determine if the input stage is unacceptably degraded.

- f. *Multiple Redundancy* - In highly redundant systems which are allowed to gracefully degrade through failures of redundant elements, a test should be established to verify that minimum acceptable system performance levels are met during system operation.
- g. *Echo Message* - When it is necessary to transmit long messages, the ability to echo back a message is particularly useful. This feature provides confidence that the message has been accurately received. A time out is usually set in anticipation of the echo message. If nothing, or if an erroneous echo is received before the time out has elapsed, the message is sent again and a fault flag is set.
- h. *System Check* - Severe and damaging faults often render it impossible for a system to check itself. One by-product of redundancy is the fact that without much complication a system that is capable of checking itself can also check out another system like itself. Therefore, it may be advantageous to have similar systems periodically check each other.
- i. *Redundant Bus* - Provision for a status word has been included successfully in 1553-type systems utilizing redundant buses. Subsystem access to the bus is completely controlled by a bus controller. Each subsystem is informed by the bus controller when to send and when to receive a message. Every time a subsystem receives such information from the bus controller, the

subsystem sends a status word back to the bus controller. This status word usually contains a number of bits reflecting the health of the subsystem, the actual word-count received, the comparison results of the expected word-count, the word-count it is presently sending, etc. If the bus monitor detects an error within the bus system, it automatically switches over to the redundant bus and reports this out upon demand. Maintenance personnel can isolate a fault quickly by observing failure indications from the bus monitor as well as from the various subsystems.

- j. *Non-Volatile RAM* - A microprocessor's ability to access a non-volatile RAM serves a dual purpose. First, it can log fault-detection information that may be retrieved by maintenance personnel after power has been shut off. Secondly, it can log software errors detected and trapped during on-line programming. A third possible service worth noting is the use of non-volatile RAMs to periodically check certain computed values. Power transient induced faults would then become tolerable because the processor would have to only "roll back" to the value stored at the checkpoint rather than begin the entire computation all over again.
- k. *Intermittent Faults* - One way to identify intermittent faults is to log every detected occurrence into memory (possibly non-volatile memory). Once the trend of an intermittent fault is determined, effective corrective action can be taken.
- l. *Signal Elements* - It is often imperative that C³I signals be sent in hostile and jamming environments. Receivers can accurately interpret a signal even if 1/8 of its total initial format is lost. Although these receivers work extremely well, higher levels of fault detection coverage would be difficult to achieve with conventional overall wraparound tests or even quick operational

checks. At close range, these systems perform perfectly without antennas or even without their power amplifiers. Elegant, localized sensitivity tests, therefore, can be built into the equipment. If the equipment is unacceptably degraded, the demodulation elements must present their own fault flag outputs.

- m. *Caution Indications* - Fault tolerance can be applied to a variety of system types, i.e., electrical, mechanical, hydraulic, environmental, etc. Regardless of the system type, it is customary to include a caution indication whenever a backup system is called into service, especially when a failure within the backup system could be hazardous to those involved.

4.2.2 Maintainability of Fault Tolerant Designs

The ability to meet fault tolerant requirements imposed upon a system is greatly influenced by its capability to detect, isolate, and repair malfunctions as they occur or are anticipated to occur. This mandates that alternate maintainability and diagnostic concepts be carefully studied and reviewed before committing to a final design approach. A maintenance plan, based upon the system's maintainability features and diagnostic capabilities, must then be developed so that it optimizes logistics resource requirements. The repair scenario should be viewed from as global a position as possible to accurately determine the true, bottom-line cost. The unscheduled Organizational (O) level maintenance, although a major part, still is only a portion of the total overall maintenance activity. Other maintenance activities include scheduled/preventive, O level inspection and service, Intermediate (I)-level maintenance, and Depot (D)-level maintenance. The cost of each level contributes to the LCC which should be the driving measure for any decision a maintenance planner makes.

Probably the most important steps a maintainability engineer must take are defining effective Maintainability and Diagnostic concepts that are capable of meeting the mission performance requirements while min-

imizing LGC. Usually, there are a handful of options available, but before one can intelligently choose the correct approach, some basic and typical questions should be answered:

- What are the overall mission reliability requirements?
- Do these requirements demand multiple redundancies and/or sophisticated techniques to enhance reliability?
- What is the system's allowable loss probability per operating hour requirement?
- What are the system performance monitoring requirements?
- What are the required maximum and mean times to repair?
- What are the risk areas that demand attention?
- Will on-line or in-flight maintenance be required or even be possible?
- What is the Fraction of Faults Isolatable (FFI) design goal?
- What percentage of the maintenance diagnostics can be achieved by the embedded diagnostics provided to meet safety and functional performance requirements?
- Can BIT eliminate and/or complement ATE requirements?
- Can the intermediate level of maintenance be minimized or eliminated?
- Can the equipment design be functionally partitioned to facilitate a module-level maintenance concept?
- Can reliance on support equipment be eliminated?
- Can the ability to record maintenance history (in-flight and on-ground) be provided within the onboard diagnostic system design?

The appropriate answers to these and other pertinent questions, will help formulate the maintainability and diagnostic concepts necessary for the system. In addition, by reviewing previous history and the available and allowable resources (such as man-hours, personnel skill levels, GSE requirement and system availability requirements), better judgments can be made on logistics decisions such as:

- How often should a corrective maintenance action be expected?

- Should the designer plan for scheduled maintenance, and if so, how often?
- How many and what types of spares should be stocked?
- Where should the spares be stocked?
- Should an instructive computer program be developed to aid the technicians involved in maintenance and fault isolation activities?

How a system is to be maintained should be analyzed in parallel with how it should be designed to meet its reliability, availability (heavily influenced by maintainability) and survivability requirements. The maintenance concept should be considered early in the design phase of the program, since there is a better chance to develop a cost-effective and efficient system if maintainability is an initial design concern.

Providing an efficient, cost effective means of maintaining a C³I system, without hindering mission performance (or affecting mission requirements), requires that a design vs. corrective maintenance trade-off analysis be conducted early in the development process. For example, to achieve a mission reliability goal with a K out of N redundant system (see para. 4.1.6), more frequent restoration of redundant elements would result in a lower number of required total redundant elements (but in higher maintenance hours). Conversely, if operational considerations dictate an extended time period between redundancy restoration, then a larger number of redundant elements would be required to satisfy the mission reliability goal. Details of design vs. corrective maintenance trades are illustrated in the *Fault Tolerant Design Implementation Guide*.

Before a decision is reached on selecting a particular redundancy scheme, contractor program managers should insure that satisfactory responses are obtained for the following typical maintenance related questions:

- What methods will be used to fault detect (FD) and fault isolate (FI)? How effective will the FD/FI tests be? What faults cannot be detected and/or isolated using the FD/FI tests?

- What is the risk that an unscheduled corrective maintenance action will adversely affect the mission? Is it tolerable?
- How many manhours would be necessary to perform anticipated unscheduled maintenance actions?
- What would be the mean-time-to-repair (MTTR) for such a system?
- Does this MTTR meet the system performance requirements?
- Can the system provide full service during an unscheduled maintenance activity (consideration must be given to power supplies, maintenance technician and tool access, possible shorting of adjacent channels, etc.)?
- How many spares must be stocked and at how many locations?
- How long does it take to replenish the spares inventory?

Table 4-3 presents attributes of some of the options available for maintaining fault tolerant C³I systems requiring high readiness levels.

4.2.3 MAINTAINABILITY AND TESTABILITY CHECKLIST QUESTIONS

Maintainability

- a. Will the Maintainability concepts be developed in parallel with other concepts proposed for achieving reliability, availability and survivability requirements?
- b. Have the costs of all the required maintenance levels been considered before presenting a maintenance concept? (C)
- c. What Maintenance concept options will best provide an efficient, cost-effective means to maintain a C³I system without hindering mission performance?

Testability/Diagnostics

- a. What resources will be required for Testability/Diagnostics to meet the fault tolerance design goals?
- b. Can the BIT and BITE design (used to detect and isolate faults for performance monitoring and maintenance) be used to achieve the desired fault tolerance performance levels?
- c. What additional constraints are imposed upon the testability/diagnostics design? (C)

TABLE 4-3. Maintenance Concept Options.

MAINTENANCE CONCEPT	DESCRIPTION	TYPICAL APPLICATIONS	ADVANTAGES	DISADVANTAGES
ON-LINE	DESIGN ALLOWS RAPID RESTORATION OF THE SYSTEM BY REPLACEMENT OF BIT/FIT IDENTIFIED LRU's AND LRM's WITH SPARES.	HIGH CRITICALITY STRATEGIC SYSTEM FUNCTIONS, I.e., DATA PROCESSING, COMMUNICATION LINKS, ETC. ALSO IN-FLIGHT ON-EQUIPMENT MAINTENANCE WITH ON-BOARD SPARES.	SYSTEM CONTINUES FULL OPERATION OR WITH MINOR INTERRUPTION IN SERVICE.	ADDED COMPLEXITY OF FD/FI, AND SWITCHING. ADDED COST OF DUPLICATED EQUIPMENT AND ON-LINE SPARES.
DEFERREL	DESIGN ALLOWS SCHEDULING NON-CRITICAL MAINTENANCE AT A MORE CONVENIENT TIME OR PLACE.	ACCEPTABLE DEGRADED MODES OF OPERATION AND OTHER GRACEFULLY DEGRADING SYSTEMS. NON-CRITICAL EQUIPMENT FAILURES.	SYSTEM CONTINUES OPERATING. MORE EFFICIENT USE OF MAINTENANCE MANPOWER AND SCHEDULE.	FULL PERFORMANCE CAPABILITY MAY NOT BE AVAILABLE, IF NEEDED.
OPPORTUNISTIC	DESIGN ALLOWS CONTINUED OPERATION WITH A DEGRADED SYSTEM UNTIL THE REQUIRED MIX OF SPARES, ATE, PERSONNEL AND SCHEDULE IS AVAILABLE TO PERFORM THE DEFERRED MAINTENANCE.	ACCEPTABLE DEGRADED MODES OF OPERATION AND OTHER GRACEFULLY DEGRADING SYSTEMS. NON-CRITICAL EQUIPMENT FAILURES.	SYSTEM MAINTAINS HIGH READINESS. MORE EFFICIENT USE OF MAINTENANCE MANPOWER AND SCHEDULE.	FULL PERFORMANCE CAPABILITY MAY NOT BE AVAILABLE, IF NEEDED.
PREPOSITIONED	COMPREHENSIVE MAINTENANCE IS LIMITED TO SPECIFIC SITES. THE SYSTEM CAN BE DIVERTED OR TRANSPORTED FROM ITS OPERATIONAL SITE TO A PARTICULAR MAINTENANCE SITE TO PERFORM A PARTICULAR LEVEL OF MAINTENANCE.	AIRBORNE C ³ I SYSTEMS AND TRANSPORTABLE SUBSYSTEMS.	REDUCED MAINTENANCE MANPOWER, SKILL LEVELS AND SUPPORT EQUIPMENT REQUIRED.	MAY RESULT IN DEGRADED READINESS.
RAPID DEPLOYMENT	DESIGN PERMITS SYSTEM OPERATION FOR A SPECIFIC TIME PERIOD WITH MINIMUM LOGISTICS AND SUPPORT RESOURCES.	GROUND MOBILE AND AIRBORNE C ³ I SYSTEMS WITH SELF-CONTAINED ELECTRICAL GENERATORS, AUXILIARY POWER UNITS, JET FUEL STARTERS, ETC.	ENHANCED TACTICAL/SURGE CAPABILITY DURING HOSTILE ACTIONS.	ADDED SYSTEM COMPLEXITY.
AUSTERE SITE	DESIGN PERMITS SYSTEM OPERATION FOR EXTENDED TIME PERIODS AT UNIMPROVED FACILITIES WITH MINIMAL LOGISTICS RESOURCES.	GROUND AND AIRBORNE C ³ I SYSTEMS WITH SELF-CONTAINED ELECTRICAL GENERATORS, AUXILIARY POWER UNITS, JET FUEL STARTERS, ETC.	ENHANCED SYSTEM SURVIVABILITY DURING HOSTILE ACTIONS.	ADDED INITIAL SYSTEM COST.
SELF CONTAINED	A SYSTEM CONTAINING SUFFICIENT FAULT TOLERANT DESIGN PROVISIONS THAT REQUIRES LITTLE OR NO EXTERNAL MAINTENANCE TO COMPLETE A MISSION.	HIGH CRITICALITY STRATEGIC NATIONAL SECURITY SYSTEMS.	HIGH READINESS.	ADDED COMPLEXITY, WEIGHT, POWER AND INITIAL COST.
R87-3537-016(T)				

- d. What recent technological advances can be used to solve testability/diagnostics design problems? (C)
- e. Can the ratio of the functional circuitry failure rate to BIT circuitry failure rate be kept above 10-to-1 as a general rule and still cover all diagnostics requirements including redundancy management? If this is not possible, is there a good reason for exceeding this goal? (C)
- f. What are the time constraints for BIT performance in the operational time line?

5 - FAULT TOLERANCE DESIGN AND TRADEOFF ANALYSES

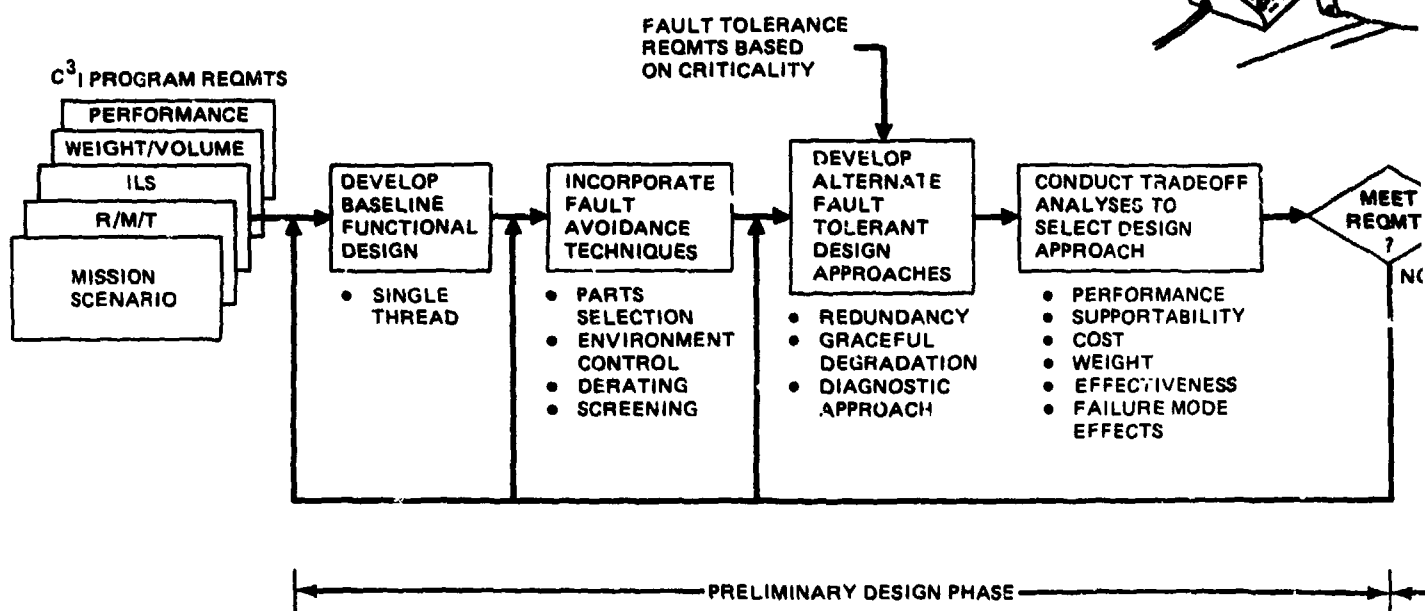
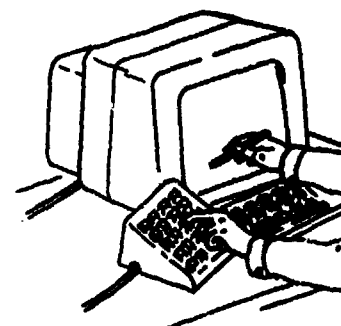
This section provides the necessary management background information to formulate fault tolerant designs and conduct tradeoff analyses. The approach described herein promotes the development of balanced designs with R/M/T attributes to enhance supportability and mission effectiveness at minimal life cycle cost.

5.1 FAULT TOLERANCE DESIGN METHODOLOGY

Fault tolerance must be incorporated into the design as part of the system engineering process. Experience has shown that a hierarchical approach, involving the selective application of fault tolerant design techniques, is most effective. Figure 5-1 shows the recommended fault tolerant design methodology. This approach consists of first creating a baseline design, and then systematically introducing fault tolerance to meet the R/M/T requirements. The process is iterative and assures that all system requirements can be achieved within program cost and schedule constraints.

5.1.1 Baseline Design

The first step in fault tolerant design process is to develop a baseline system architecture for the implementation technology that meets the system performance requirements. This first cut architecture should be non-redundant, i.e., contain only the minimum hardware complement needed to meet the performance parameters. Furthermore, technology used in the baseline design must represent a reasonable and attainable development risk that is consistent with the program cost and schedule constraints. The use of high risk technology that is incompatible with program cost and schedule will inevitably result in serious R/M/T and system performance deficiencies.



R87-5011-501
R87-3537-017(T)

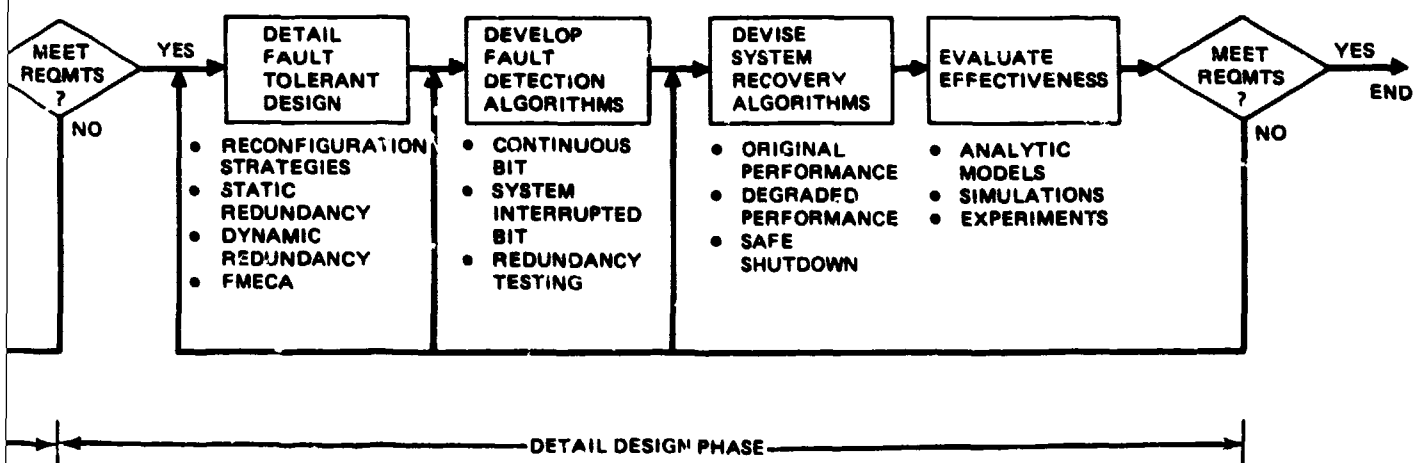


Figure 5-1. Fault Tolerance Design Methodology.

5.1.2 Fault Avoidance Techniques

While the baseline design is being developed, applicable fault avoidance techniques should be identified and carefully evaluated. These techniques normally represent the most cost effective method of increasing system reliability. Typically they include the following approaches:

- Reduction of environmental stresses, e.g., providing increased cooling and/or vibration isolation. For operating temperatures between 10°C and 50°C, a 10 to 15 percent increase in reliability can be expected for each 10°C decrease in temperature
- Use of military grade piece parts instead of commercial grade
- Application of a more stringent part derating policy for new designs
- Imposition of environmental stress screening at the piece part and equipment levels.

5.1.3 Development of the Fault Tolerant Design Approach

Section 3 of this Guide describes the methodology used to establish the system fault tolerance requirements based on mission and safety criticalities. In addition to these contractor-developed requirements, the Air Force imposes R/M/T and availability requirements which significantly influence the selection of fault tolerant configurations. Fault tolerance requirements are allocated by contractor personnel to each hardware element in the system. This assures that fault tolerant design emphasis is directed at the critical areas and not indiscriminately across the entire system. Compliant design approaches can then be formulated using the various fault tolerant options discussed in Section 4 of this Guide.

Typically, three to four designs are initially configured and qualitatively evaluated against the major system drivers, i.e., performance; cost, weight, supportability, etc. Normally, the two most promising candidate approaches are selected for further configuration definition and tradeoff analysis. Alternate testability/diagnostic concepts must be concurrently developed and included as part of the design tradeoff process. System level FMECAs should be conducted on each alternate candidate

configuration to identify single point failures and other potential design weaknesses impacting safety and reliability. Paragraph 5.2 describes the analysis methods that are commonly used to evaluate design alternatives and select the most desirable design approach prior to the Preliminary Design Review (PDR). Design trades should continue long after the PDR and focus on the detail design issues.

5.1.4 Fault Detection Implementation

After establishing the system diagnostic approach, appropriate fault detection techniques must be defined to detect all relevant fault types in a timely manner. Fault detection algorithms are implemented via various hardware, software, and repetition (time) methods to generate the initial fault signal. Fault detection algorithms are classified in accordance with the time of their application as follows:

- *Continuous (Background) or Non-Interference Testing* - Simultaneous with normal system operation
- *System Interrupted Testing* - After normal operation has been temporarily interrupted
- *Redundancy Testing* - Either concurrently or at scheduled intervals; verifies that the various forms of protective redundancy are themselves fault-free
- *Validation Testing* - Identifies system imperfections introduced during the manufacturing and programming processes prior to system deployment.

5.1.5 Recovery Implementation

After a fault is detected, recovery algorithms are used to reconfigure the system to an alternate mode of operation or safely shut the system down. Examples of reconfiguration include: deactivating a failed processor and switching in a standby spare processor, deactivating a faulty memory area and reallocating the remaining available storage area of the memory. The anticipated extent of hardware damage as a result of a fault and the time required to resume system operation have a major influence on the choice of recovery techniques that can be used. Fault

signal-invoked recovery algorithms are classified according to the state of the system after recovery as follows:

- Recovery to original performance
- Recovery to degraded modes of system operation
- Execution of a safe shutdown.

5.1.6 R/M/T Evaluation Techniques

The design activity must be supported by a continual assessment of the system's ability to meet the R/M/T and availability requirements. Current and future C³I systems will utilize extensive redundancy, as well as, complex fault detection and recovery management techniques. The trend towards these ultra-reliable fault tolerant systems has necessitated the development of sophisticated R/M/T evaluation tools.

In the past, the lack of redundancy was felt to be the major source of system unreliability and imperfect fault protection coverage was deemed to have only a second-order effect. With the increased emphasis on fault tolerance for present day C³I systems, redundancy and fault protection coverage have achieved at least parity, if not complete role-reversal. System faults which occur may or may not be detected, and faults which are detected may or may not result in correct isolation and reconfiguration. Thus, to be of value, analytical reliability and availability models must properly account for the adverse effects of imperfect fault protection coverage. System reliability and availability figures of merit must be determined by evaluating the inherent fault protection coverage and the ability to reconfigure to alternate modes of acceptable system operation.

To date, most of the reliability models used to evaluate complex fault tolerant systems are based on Markov methods. Some of the more popular models are ARIES, CARE III, HARP and SURE and their important characteristics are summarized in Table 5-1. The reader should refer to the *Fault Tolerant Design Implementation Guide* for more information on this subject.

TABLE 5-1. Characteristics of Current Reliability Models.

ATTRIBUTE	MODEL			
	APRS	CARE II	HARP	SURE
SIZE	LARGE SYSTEMS	LARGE SYSTEMS	SMALL SYSTEMS	SMALL SYSTEMS
MATURITY	MATURE	MATURE	RELATIVELY NEW	RELATIVELY NEW
RESULT	LOWER BOUND	LOWER BOUND	LOWER BOUND	UPPER & LOWER BOUNDS
SOLUTION	EIGENVALUE	NUMERICAL INTEGRATION	NUMERICAL INTEGRATION	NEW ALGEBRAIC THEORY
MODEL TYPE	HOMOGENEOUS MARKOV	SEMI-MARKOV	NON-HOMOGENEOUS MARKOV	SEMI-MARKOV
INPUT	SYSTEM STATE	FAULT TREE	FAULT TREE OR SYSTEM STATE	SYSTEM STATE
REPAIRABLE SYSTEM	YES	NO	YES	NO
FAILURE RATES	EXPONENTIAL	EXPONENTIAL OR WEIBULL	WEIBULL FOR NON-REPAIRABLE SYSTEMS	EXPONENTIAL
FAULT HANDLING	INSTANTANEOUS CONSTANT FAULT PROTECTION COVERAGE F. CTORS ARE INPUT	INCLUDES A SEPARATE MODEL WHICH IS INDEPENDENT OF SYSTEM STATE	CHOICE OF 7 MODELS, ONE OF WHICH IS A SIMULATION	NO DETAILED PARAMETRIC MODEL. INPUT SAMPLE MEANS AND VARIANCES OF RECOVERY.
SPARES	SPARES HAVE OWN FAILURE RATES	HOT WITH SAME FAILURE RATE AS ACTIVE UNITS	SPARES HAVE OWN FAILURE RATES	WHEN COLD, FAILURE RATE IS ZERO. WHEN HOT, SAME FAILURE RATE AS ACTIVE UNITS.
R87-3537-018(T)				

5.1.7 FAULT TOLERANT DESIGN METHODOLOGY CHECKLIST QUESTIONS

The following questions are intended to assist program managers in achieving the appropriate level of fault tolerance through the design and tradeoff analysis process:

- Does the systems design approach include fault tolerance as an integral part of the systems engineering process?
- Does the system design approach clearly reflect the R/M/T and fault tolerance requirements and the methods for their evaluation and optimization?
- What is the overall diagnostic strategy?
- What is the system level fault protection design concept?

- e. What analyses/tradeoffs have been accomplished, or are planned to assure a system architecture that minimizes the effect of faults?
- f. What are the fault containment strategies? How is data integrity, including data bases, protected from damage caused by faults?
- g. What is the software overhead penalty for implementing fault tolerance? What is the hardware penalty for implementing fault tolerance techniques?
- h. How are the fault tolerant system interfaces protected?
- i. Has a list been developed of all the critical technology developments needed to support fault tolerance? What are the states of development of these technologies?
- j. How credible is the reliability/availability model and supporting input data?

5.2 R/M/T DESIGN TRADEOFF ANALYSES

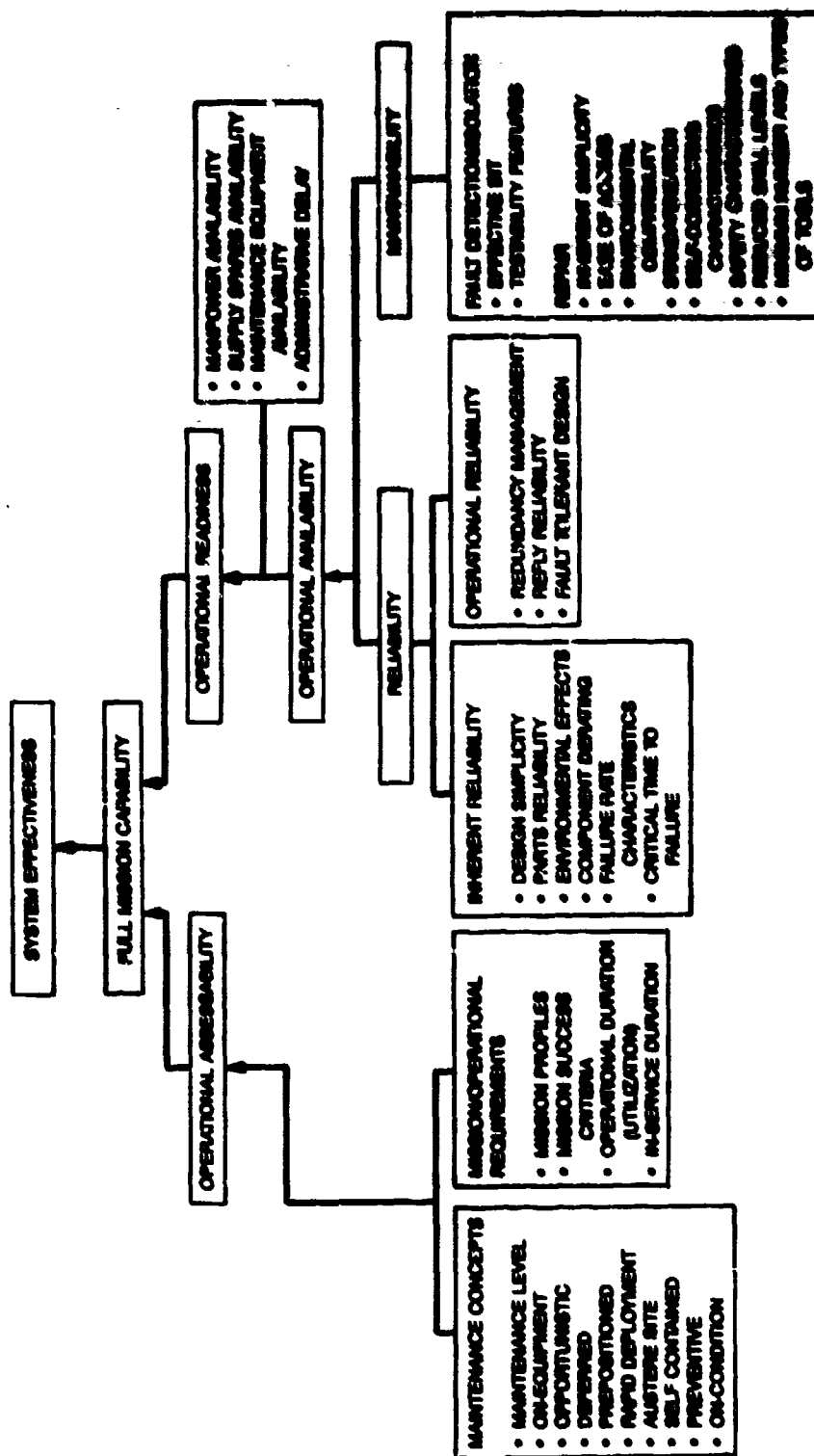
5.2.1 Readiness Analysis

Readiness tradeoff analyses are used to evaluate the impact of R/M/T design features in conjunction with the operational and mission requirements of the system. Readiness is defined as the probability that a system is either operational or ready to be placed into operation at any point in time. The major factors that influence readiness are:

- Reliability and maintainability design characteristics
- Field maintenance concept employed
- Logistic resources available
- Mission and operational requirements.

These factors and relationships affecting readiness are shown in Fig. 5-2.

The readiness of a weapon system is primarily dependent upon the "repairability" characteristics of the design, i.e., the ability to accom-



RS7-3837-019(T)

Figure 5-2. Factors & Relationships Affecting Readiness & System Effectiveness.

plish corrective and preventive maintenance within a prescribed period of "downtime." This is expressed by the availability (readiness) ratio:

$$\text{Availability (readiness)} = \frac{\text{Uptime}}{\text{Uptime} + \text{Downtime}}$$

The terms, *operational availability* (A_o) and *readiness*, are essentially interchangeable. Uptime is a function of the maintenance interval or mean-time-between-maintenance (MTBM). Downtime is determined by the mean restore time (MRT) to return the system to operational status. Therefore, operational availability is expressed in the following equation:

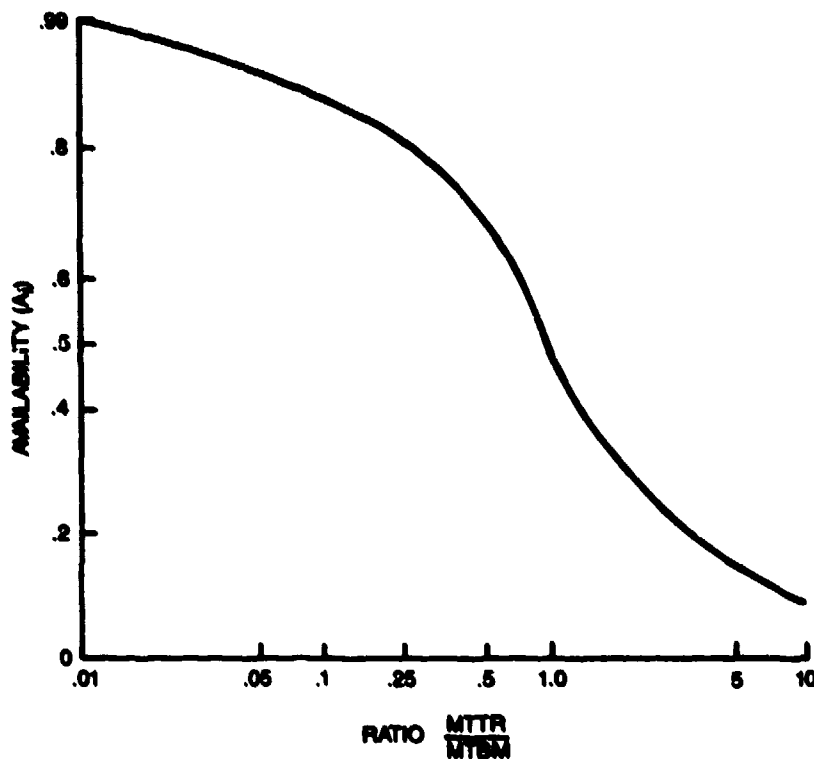
$$A_o = \frac{\text{MTBM}}{\text{MTBM} + \text{MRT}}$$

The maintenance interval comprises all the maintenance actions associated with functional failures, scheduled maintenance, inspections, cannibalizations and false alarms. The MRT includes the actual mean-time-to-repair (MTTR) a system coupled with the elapsed time associated with logistic supply and manpower delays. MTBM and MTTR are determined by the system's design features. Supply and awaiting maintenance delays are caused by logistic resource deficiencies which can be minimized with effective management and planning. Therefore, system readiness, directly attributable to design characteristics, is normally evaluated in the design phase using the classical steady-state *inherent* availability (A_i) relationship:

$$A_i = \frac{\text{MTBM}}{\text{MTBM} + \text{MTTR}}$$

The reliability, maintainability and testability attributes are evaluated through design tradeoffs which achieve a balance of supportability

features with the operational and mission needs, and program resources. As the maintenance interval is increased through improved reliability, the inherent availability of a system will approach 100%. Similarly, maintainability design improvements can reduce the number of false alarms and expedite maintenance. This improves the availability of the system by increasing the interval between maintenance (MTBM) and reducing the MTTR. The availability ratio, MTTR/MTBM, is used extensively in design tradeoffs to assess the reliability, maintainability and testability impact on system availability, as illustrated in Fig. 5-3. As this ratio decreases, either through an increase in the maintenance interval or reduction in the restore time, the system availability/readiness improves.



R87-3537-020 (T)

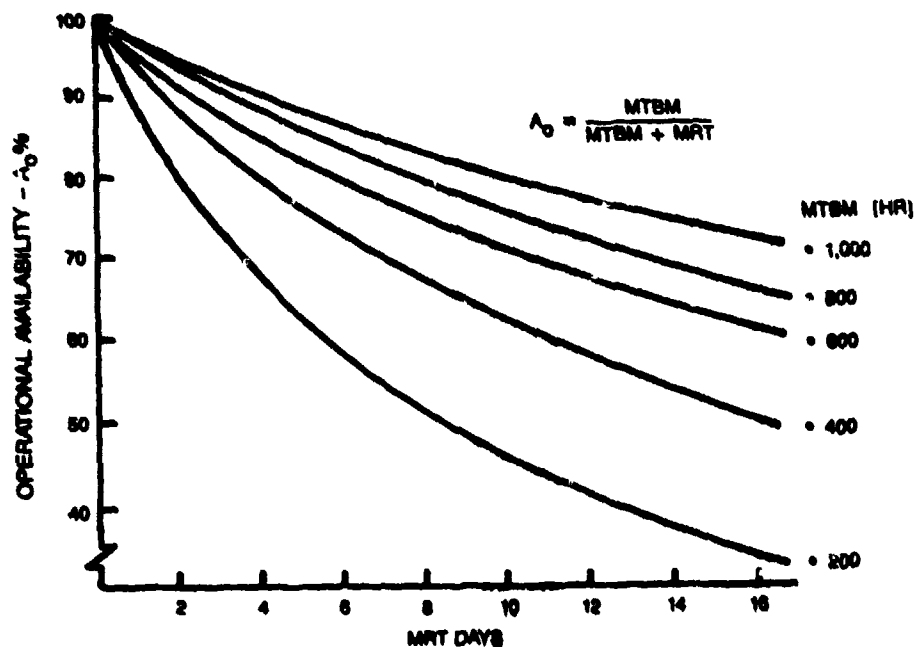
Figure 5-3. Relationship of Availability and Its Drivers MTTR & MTBM.

Utilization is an important consideration for systems that are subjected to long periods of inactivity and brief actual operating times.

With fixed logistic assets available, an increase in system utilization taxes the maintenance resources and decreases system readiness.

5.2.2 Logistics Resource Analysis

Effective management of logistic resources (personnel, facilities, equipment and spares) is essential to achieve a high state of system readiness. Program managers must allocate sufficient funds to establish logistic requirements and purchase the necessary logistic resources. Even highly reliable systems, when they fail, can suffer rapid degradation in system readiness. To avoid deterioration of a system's readiness capability, logistic planners must provide properly trained maintenance personnel, facilities and test equipment to accomplish maintenance, and sufficient quantities of replacement parts and materials. Figure 5-4 shows how a system's operational availability (A_o) will decay with increasing restore time due to delays in logistic supply and maintenance personnel.



R87-351 7-022(T)

Figure 5-4. Relationships of A_o , Reliability, & MRT.

Maintenance manpower requirements are based on the number and types of skills required to perform the repair and scheduled maintenance tasks at the anticipated maintenance frequencies. The spares requirements for a program are normally determined by performing a level of repair analysis as part of the Logistic Support Analysis (LSA) activity. This analysis establishes the most economic level of repair (assembly, subassembly, component) and identifies where the repair should be accomplished (organization, intermediate, depot) based on the maintenance concept. Logistic downtime is highly dependent upon the level of repair, the repair facility and the number of spares available.

5.2.3 Mission Effectiveness Analysis

Mission effectiveness, $E(t)$ is a measure of a system's capability to accomplish its mission objectives within the stated operational demand time. $E(t)$ is expressed as the product of the operational availability (A_o), mission reliability ($R(t)$) and the system performance index P_s as follows:

$$E(t) = A_o R(t) P_s$$

This expression takes into account the probability that the system will be available on operational demand (A_o), the probability of not experiencing a critical system failure ($R(t)$), and the percentage of mission objectives that can be expected to be accomplished (P_s). For a C³I system, the system performance index would relate the mission objectives to system capabilities such as, area of surveillance, target detection probability, etc. The availability, reliability and performance parameters are defined in terms of the normal and degraded modes of system operation. Configuration trades affecting reliability, supportability and readiness can then be evaluated as a function of mission effectiveness.

5.2.4 Life-Cycle Cost (LCC) Analysis

Tradeoffs are not meaningful unless they can be expressed in terms of a common parameter. In terms of readiness, cost is the best common

denominator for normalizing the effects of all the diverse variables associated with R/M/T and logistics. As an example, the maintainability characteristics of a C³I system can be quantified in terms of acquisition and operating and support (O&S) costs by identifying the impacts on prime equipment, personnel, support equipment, spares, publications, etc. However, the cost impact of having a multi-million dollar system unavailable for a mission is difficult to measure. It is therefore convenient to evaluate a system in terms of weapon system ready-hours. By addressing the problem on a total-force-level basis, it can be shown that a few weapon systems with a high readiness rate can be as effective as a larger number of weapon systems with a lower readiness rate. A break-even point will define when it is more cost-effective to procure additional weapon systems, rather than incorporate additional readiness improvements.

It is sometimes advantageous to work with a worth value rather than cost directly. Costs can be converted to the worth of a ready-hour by dividing the anticipated LCC of the weapon system by the number of ready-hours (requirement or goal) during the life-cycle of the system. The relationship is:

$$R_I = \frac{\text{LCC Per System}}{R \times SL \times 365 \text{ Days/Yr.} \times 24 \text{ Hrs./Day}} = \frac{\text{Total Dollars}}{\text{Ready-Hours}}$$

where:

R_I = Readiness Index = Worth of a Ready-Hour

R = Readiness Rate

and SL = Service Life (Yrs.)

Using the readiness criteria, any improvement to the system can be evaluated on a cost effectiveness basis. As an example, for a system with a readiness goal of 80%, a service life of 20 years, and an anticipated LCC of \$75,000,000 per weapon system, a readiness index of

\$535/Ready-Hour is obtained. For this particular system, if the cost of saving one ready-hour over its service life exceeds \$535 the improvement should not be implemented.

5.2.5 R/M/T DESIGN TRADEOFF ANALYSIS CHECKLIST QUESTIONS

- a. Have probabilistic and quantitative readiness goals and requirements been defined? (PA)
- b. Have system utilization, on-station demand, and critical turn-around requirements been quantified? (PA)
- c. Have the following factors been considered in developing specific operational, maintenance and support requirements?
 - Facility needs
 - Manpower constraints and loading
 - Maintenance state of the art
 - System support concept
 - Levels of repair
 - Provisioning and stock-out levels
 - Special support equipment and diagnostic test architecture
 - Maintenance publication and training
 - Special and readiness inspections
- d. Are logistic support cost, LCC, level of maintenance, and mission simulation model requirements defined in support of system readiness trades and effectiveness analysis?
- e. Has provision been made to use results of readiness analysis for:
 - Support of design trades?
 - Optimization of support systems?
 - Progress towards meeting system demand requirements?
 - Identifying readiness risks?
- f. Are reliability and maintainability quantitative requirements adequately defined at all levels (system, subsystem, component, etc.) to ensure necessary quantitative readiness assessments?
- g. Are warranties and/or contractor maintenance factors contained in the readiness equations? If so, how are they to be implemented?

6 - ACRONYMS

A/D	Analog to Digital
AF	Air Force
ARIES	Automated Reliability Interactive Estimation System (Computer Program)
ATE	Automatic Test Equipment
AWACS	Airborne Warning And Control System
BIT	Built-In Test
BITE	Built-In Test Equipment
C	Contractor
CARE	Computer Aided Reliability Estimation (Computer Program)
C³I	Command, Control, Communications and Intelligence
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CONCEPT	Concept Exploration (Phase)
COTS	Commercial Off-the-Shelf
CPU	Central Processing Unit
D	Depot
DoD	Department of Defense
DSP	Defense Support Program
ECP	Engineering Change Proposal
ESS	Environmental Stress Screening

FD	Fault Detection
FFI	Fraction of Faults Isolatable
FI	Fault Isolation
FMEA	Failure Mode Effects Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
FRACAS	Failure Reporting, Analysis and Corrective Action System
FSD	Full Scale Development (Phase)
FSED	Full Scale Engineering Development (Phase)
GSE	Ground Support Equipment
HARP	Hybrid Automated Reliability Predictor (Computer Program)
I	Intermediate
ILS	Integrated Logistic Support
IMU	Inertial Measurement Unit
IR	Infrared
Joint STARS	Joint Surveillance Target Attack Radar System
LCC	Life-Cycle Cost
LRM	Line Replaceable Module
LRU	Line Replaceable Unit
LSA	Logistic Support Analysis
MRT	Mean Restore Time
MTBCF	Mission-Time-Between-Critical-Failure
MTBF	Mean-Time-Between-Failure
MTBMA	Mean-Time-Between-Maintenance-Action
MTBMI	Mean-Time-Between-Maintenance-Inherent
MTTR	Mean-Time-To-Repair

NMR	N-Modular Redundancy
O	Organizational
O&S	Operating and Support
PA	Procuring Activity
PDR	Preliminary Design Review
PM	Preventive Maintenance
PROD	Production and Deployment (Phase)
R&M	Reliability and Maintainability
RAM	Random Access Memory
RF	Radio Frequency
RFP	Request For Proposal
RIW	Reliability Improvement Warranty
R/M/T	Reliability, Maintainability, Testability
RQT	Reliability Qualification Test
SOW	Statement of Work
SRR	System Requirements Review
SRU	Shop Replaceable Unit
ST	Self-Test
SURE	Semi-Markov Unreliability Range Evaluator (Computer Program)
TMR	Triple Modular Redundancy
TPS	Test Program Set
VALID	Demonstration and Validation (Phase)
VHSIC	Very High Speed Integrated Circuit
VLSI	Very Large Scale Integration

APPENDIX A

GLOSSARY OF RELIABILITY, MAINTAINABILITY, TESTABILITY AND FAULT TOLERANCE TERMS

APPENDIX A

GLOSSARY OF RELIABILITY, MAINTAINABILITY, TESTABILITY AND FAULT TOLERANCE TERMS

AVAILABILITY: A measure of the degree to which an item is in an operable and committable state at the start of a mission when the mission is called for at an unknown (random) time. (Item state at start of a mission includes the combined effects of readiness-related system reliability and maintainability parameters, but excludes mission time.) (1)

COVERAGE, FAULT PROTECTION: The conditional probability that the system will recover should a fault occur.
The specification of the types of errors against which a particular redundancy scheme guards. (2)

DEPENDABILITY: A measure of the degree to which an item is operable and capable of performing its required function at any (random) time during a specified mission profile, given item availability at the start of the mission. (Item state during a mission includes the combined effects of reliability and maintainability parameters but excludes mission time.) (1)

ERROR: An undesired resource state that exists either at the boundary or at an internal point in the resource and may be perceived as a failure when it is propagated to and manifested at the boundary.
(3)

FAILURE: The event, or inoperable state, in which any item or part of an item does not, or would not, perform as previously specified. (1). A loss of service that is perceived by the user at the boundary of the resource. (3)

FAULT: The immediate cause of failure (e.g., mal-adjustment, misalignment, defect, etc.) (1). The identified or hypothesized cause of the error or failure. (3). A fault may be latent and undetected until it propagates and causes an error or functional failure at a higher level of operation.

FAULT, DESIGN: A generic fault designed into a function, including hardware and software faults and faults of other logical entities, such as data bus interfaces.

FAULT DETECTION: The process of determining that an error caused by a fault has occurred within the system. An undiscovered fault is classified as a latent fault.

FAULT, INTERMITTENT: Hardware faults which result in recurring inconsistent functional behavior of the hardware followed by recovery of its ability to perform within specified limits without any remedial action. Intermittent faults cannot occur in software or logic.

FAULT ISOLATION: The process of determining the location of a fault to the extent necessary to effect repair, correction, or restoration to specified performance. (1)

FAULT, LATENT: A fault which exists but has not been detected.

FAULT, PERMANENT: A fault which, once it occurs, is irreversible

except for permanent removal from the system.

FAULT RECOVERY: The ability of the system to provide the required service or performance or to correct errors after a fault has been detected.

FAULT, TRANSIENT: A fault not caused by a permanent defect but rather one which manifests a faulty behavior for some finite time and then is fault free. A permanent or intermittent fault which only occasionally produces discrepant results is not a transient fault.

FAULT TOLERANCE: A survivable attribute of a system that allows it to deliver its expected service after faults have manifested themselves within the system. (3)

FAULT TOLERANT SYSTEM: A system that has provisions to avoid failure after faults have caused errors within the system. (3)

ITEM: A generic term which may represent a system, subsystem, equipment, assembly, subassembly, etc. depending on its designation in each task. (4)

MAINTAINABILITY: The measure of the ability of an item to be retained in or restored to specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair. (1)

MEAN-TIME-BETWEEN-FAILURE (MTBF): A basic measure of the system reliability parameter related to availability and readiness. The total number of system life units, divided by the total number of events

in which the system becomes unavailable to initiate its mission(s), during a stated period of time. (1)

MISSION-TIME-BETWEEN-CRITICAL-FAILURES (MTBCF): A measure of **MISSION RELIABILITY:** The total amount of mission time divided by the total number of critical failures during a stated series of missions. (1)

OPERABLE: The state of being able to perform the intended function. (1)

REDUNDANCY: The existence of more than one means of accomplishing a given function. Each means of accomplishing the function need not necessarily be identical. (1)

REDUNDANCY, ACTIVE: The redundancy wherein all redundant items are operating simultaneously. (1)

REDUNDANCY, STANDBY: That redundancy wherein the alternative means of performing the function is not operating until it is activated upon failure of the primary means of performing the function. (1)

RELIABILITY: (a) The duration or probability of failure-free performance under stated conditions. (1).

(b) The probability that an item can perform its intended function for a specified interval under stated conditions. (For non-redundant items this is equivalent to definition (a). For redundant items this is equivalent to the definition of mission reliability.) (1)

RELIABILITY, MISSION: The ability of an item to perform its required

functions for the duration of the specified mission profile. (1)

TESTABILITY: A design characteristic which allows the status (operable, inoperable, or degraded) of an item to be determined and the isolation of faults within the item to be performed in a timely manner. (4)

NOTE: The sources of key definitions are given in parentheses following the definition. The source identification codes are:

- (1) MIL-STD-721C, "Definition of Terms for Reliability and Maintainability."
- (2) D. P. Siewiorek, R. S. Swarz, "The Theory and Practice of Reliable System Design", Digital Press, 1982.
- (3) A. Avizienis, J. C. Laprie, "Dependable Computing: From Concepts to Design Diversity", Proceedings of the IEEE, Vol. 74, No. 5, May 1986.
- (4) MIL-STD-2165, "Testability Program for Electronic Systems and Equipment."

APPENDIX B

REFERENCES

&

LIST OF GOVERNMENT DOCUMENTS

APPENDIX B

REFERENCES

- (1) Caroli, J. A., et al., "Reliability Demonstration Technique for Fault Tolerant Systems". *Proceedings Annual Reliability and Maintainability Symposium*, 1987 January, 316-320.
- (2) Musson, T. A., "System R&M Parameters from DoD Directive 5000.40." *Proceedings Annual Reliability and Maintainability Symposium*, 1981
- (3) National Security Industrial Association, Integrated Diagnostics Group. "Guidelines for Preparation of Diagnostic Requirements", July 21, 1986.

LIST OF GOVERNMENT DOCUMENTS

DoD Directive 5000.40	Reliability and Maintainability
DoD-STD-2167	Defense System Software Development
MIL-HDBK-338	Electronic Reliability Design Handbook
MIL-STD-470A	Maintainability Program for Systems and Equipment
MIL-STD-471A	Maintainability Verification/Demonstration/Evaluation
MIL-STD-756B	Reliability Modeling and Prediction
MIL-STD-781C	Reliability Design Qualification and Production Acceptance Tests: Exponential Distribution
MIL-STD-785B	Reliability Program for Systems and Equipment Development and Production

MIL-STD-882B	System Safety Program Requirements
MIL-STD-1388/1A	Logistics Support Analysis
MIL-STD-1521B	Technical Reviews and Audits for Systems, Equipment, and Computer Software
MIL-STD-1574A	System Safety Program for Space and Missile Systems
MIL-STD-2165	Testability Program for Electronic Systems and Equipment
NHB 1700.7A	Safety Policy and Requirements (NASA Publication)